

DOCKET NO.: 262954US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Tomoyuki ASANO

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/06324

INTERNATIONAL FILING DATE: April 30, 2004

FOR: DATA PROCESSING METHOD, PROGRAM OF SAME, AND APPARATUS AND
RECORDING MEDIUM OF SAME**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents
Alexandria, Virginia 22313

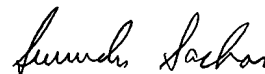
Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2003-125968	30 April 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/06324. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599 _____
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

Rec'd PCT/PTO 28 DEC 2004

PCT/JP 2004/006324

30. 4. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

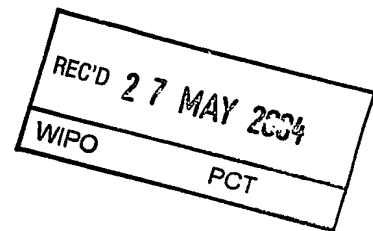
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 4 月 3 0 日

出 願 番 号
Application Number: 特 願 2 0 0 3 - 1 2 5 9 6 8
[ST. 10/C]: [J P 2 0 0 3 - 1 2 5 9 6 8]

出 願 人
Applicant(s): ソニー株式会社

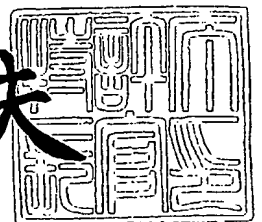


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 2 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390190928

【提出日】 平成15年 4月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06C 1/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 浅野 智之

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100094053

 【弁理士】

 【氏名又は名称】 佐藤 隆久

【手数料の表示】

 【予納台帳番号】 014890

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9707389

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理方法、そのプログラム、その装置および記録媒体

【特許請求の範囲】

【請求項 1】

記録媒体を識別する識別データを生成するデータ処理方法であって、
前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の工程と、

前記第 1 の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第 2 の工程と
を有するデータ処理方法。

【請求項 2】

前記第 1 の工程において、複数の異なる第 1 のデータの各々について、当該第 1 のデータと、前記秘密鍵データと、所定の第 2 のデータとを用いて、前記秘密鍵データに対応する公開鍵データを基に前記第 2 のデータを生成可能な前記複数の署名データを生成し、

前記第 2 の工程において、前記第 1 の工程で生成した前記複数の署名データの各々について、当該署名データと前記第 2 のデータとを含む前記識別データを生成し、当該識別データを前記記録媒体に割り当てる

請求項 1 に記載のデータ処理方法。

【請求項 3】

記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の手順と、

前記第 1 の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第 2 の手順と
を有するプログラム。

【請求項 4】

記録媒体を識別する識別データを生成するデータ処理装置であって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第 1 の手段と、

前記第 1 の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てて第 2 の手段とを有するデータ処理装置。

【請求項 5】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程

を有するデータ処理方法。

【請求項 6】

前記工程は、

前記識別データに含まれる前記署名データから、前記公開鍵データを用いて第 1 のデータを生成する第 1 の工程と、

前記識別データに含まれる第 2 のデータと、前記第 1 の工程で生成した前記第 1 のデータとを比較し、当該比較の結果を基に、前記識別データの正当性を検証する第 2 の工程と

を有する請求項 5 に記載のデータ処理方法。

【請求項 7】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順

を有するプログラム。

【請求項 8】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を

検証する手段

を有するデータ処理装置。

【請求項 9】

記録媒体を識別する識別データを生成するデータ処理方法であって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成する第 1 の工程と、

前記第 1 の工程で生成した前記複数の署名データの各々について、当該署名データと前記データ S とを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てする第 2 の工程と

を有するデータ処理方法。

【請求項 10】

前記データ S を暗号化鍵として暗号化した暗号データと、前記識別データとを前記記録媒体に書き込む第 3 の工程

をさらに有する請求項 9 に記載のデータ処理方法。

【請求項 11】

記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成する第 1 の手順と、

前記第 1 の手順で生成した前記複数の署名データの各々について、当該署名データと前記データ S とを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てする第 2 の手順と

を有するプログラム。

【請求項 12】

記録媒体を識別する識別データを生成するデータ処理装置であって、

前記識別データの管理元の秘密鍵データとデータ S とを用いて、前記管理元の公開鍵データを基に前記データ S を復号可能な複数の異なる署名データを生成す

る第1の手段と、

前記第1の手段で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てて第2の手段とを有するデータ処理装置。

【請求項13】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の工程と、

前記第1の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の工程と

を有するデータ処理方法。

【請求項14】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手順と、

前記第1の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手順と

を有するプログラム。

【請求項15】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名デー

タから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手段と、

前記第1の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手段と

を有するデータ処理装置。

【請求項16】

公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 $p(w)$ の積とし、wを $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体STM(w)の各々に割当てる識別データID(w)を生成するデータ処理方法であって、

$(KT/p(w) \bmod M)$ を算出する第1の工程と、

$p(w)$ と前記第1の工程で算出した $(KT/p(w) \bmod M)$ とを含む識別データID(w)を、記録媒体STM(w)に割当てる第2の工程と

を有するデータ処理方法。

【請求項17】

$(KT \bmod M)$ を暗号化鍵として暗号化した暗号データと、前記識別データID(w)とを前記記録媒体STM(w)に書き込む第3の工程

をさらに有する請求項16に記載のデータ処理方法。

【請求項18】

公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 $p(w)$ の積とし、wを $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体STM(w)の各々に割当てる識別データID(w)を生成するデータ処理装置が実行するプログラムであって、

$(KT/p(w) \bmod M)$ を算出する第1の手順と、

$p(w)$ と前記第1の手順で算出した $(KT/p(w) \bmod M)$ とを含む識別データID(w)を、記録媒体STM(w)に割当てる第2の手順と

を有するプログラム。

【請求項19】

公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 p (w) の積とし、 w を $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体STM (w) の各々に割当てて識別データID (w) を生成するデータ処理装置であって、

($K^T / p(w) \bmod M$) を算出する第1の手段と、
 $p(w)$ と前記第1の手段が算出した ($K^T / p(w) \bmod M$) とを含む識別データID (w) を、記録媒体STM (w) に割当てて第2の手段とを有するデータ処理装置。

【請求項20】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータ p が素数であるか否かを検証する第1の工程と、

前記第1の工程で前記データ p が素数であると検証された場合に、前記識別データに含まれるデータIDKeyと前記データ p と公開されているデータMとを用いて ($IDKey \cdot p \bmod M$) を算出する第2の工程と、

前記第2の工程で算出した ($IDKey \cdot p \bmod M$) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の工程とを有するデータ処理方法。

【請求項21】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータ p が素数であるか否かを検証する第1の手順と、

前記第1の手順で前記データ p が素数であると検証された場合に、前記識別データに含まれるデータIDKeyと前記データ p と公開されているデータMとを用いて ($IDKey \cdot p \bmod M$) を算出する第2の手順と、

前記第2の手順で算出した ($IDKey \cdot p \bmod M$) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の手順と

を有するプログラム。

【請求項 2 2】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データに含まれるデータ p が素数であるか否かを検証する第 1 の手段と、

前記第 1 の手段が前記データ p が素数であると検証した場合に、前記識別データに含まれるデータ $IDKey$ と前記データ p と公開されているデータ M とを用いて $(IDKey \cdot p \bmod M)$ を算出する第 2 の手段と、

前記第 2 の手段が算出した $(IDKey \cdot p \bmod M)$ を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第 3 の手段と

を有するデータ処理装置。

【請求項 2 3】

素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当てる識別データ $ID(w)$ を生成するデータ処理方法であって、

巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S \cdot d(w) \bmod M)$ を算出する第 1 の工程と、

前記 $e(w)$ と前記第 1 の工程で算出した $(S \cdot d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てる第 2 の工程と

を有するデータ処理方法。

【請求項 2 4】

上記データ S を暗号鍵として用いて暗号化された暗号データと、前記識別データ $ID(w)$ とを前記記録媒体 $STM(w)$ に書き込む第 3 の工程

をさらに有する請求項 2 3 に記載のデータ処理方法。

【請求項 2 5】

素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理装置が実行するプログラムであって、

巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S^{d(w)} \bmod M)$ を算出する第 1 の手順と、

前記 $e(w)$ と前記第 1 の手順で算出した $(S^{d(w)} \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てて第 2 の手順とを有するプログラム。

【請求項 26】

素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理装置であって、

巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S^{d(w)} \bmod M)$ を算出する第 1 の手段と、

前記 $e(w)$ と前記第 1 の手段が算出した $(S^{d(w)} \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てて第 2 の手段とを有するデータ処理装置。

【請求項 27】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータ e およびデータ I と公開されているデータ M とを用いて $(I^e \bmod M)$ を算出する第 1 の工程と、

前記第1の工程で算出した ($I^e \bmod M$) を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の工程とを有するデータ処理方法。

【請求項28】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータ e およびデータ I と公開されているデータ M と用いて ($I^e \bmod M$) を算出する第1の手順と、

前記第1の手順で算出した ($I^e \bmod M$) を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手順とを有するプログラム。

【請求項29】

記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データに含まれるデータ e およびデータ I と公開されているデータ M と用いて ($I^e \bmod M$) を算出する第1の手段と、

前記第1の手が算出した ($I^e \bmod M$) を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手段とを有するデータ処理装置。

【請求項30】

データを記録する記録媒体であって、

前記記録媒体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録した記録媒体。

【請求項31】

データを記録する記録媒体であって、

前記記録媒体の管理元の公開鍵データを用いて第1のデータを生成するために用いられる署名データと、前記第1のデータと比較して識別データの正当性を検証するために用いられる第2のデータとを含み前記記録媒体を識別する前記識別

データを記録した
記録媒体。

【請求項 32】

暗号データを記録する記録媒体であって、
素数であるデータ p と、
前記暗号データを復号するために用いられるコンテンツ鍵データである (ID
 $KeyP \bmod M$) を前記データ p と公開されているデータ M と共に算出する
ために用いられるデータ $IDKey$ と
を含み前記記録媒体を識別する識別データを記録した
記録媒体。

【請求項 33】

暗号データを記録する記録媒体であって、
前記暗号データを復号するために用いられるコンテンツ鍵データである (Ie
 $\bmod M$) を、公開されているデータ M と共に算出するために用いられるデー
タ e およびデータ I とを含み前記記録媒体を識別する識別データを記録した
記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記録媒体を識別する識別データに係わる処理を行うデータ処理方法
、そのプログラム、その装置および記録媒体に関する。

【0002】

【従来の技術】

光ディスクなどの記録媒体を用いてコンテンツを提供する場合に、その記録媒
体が不正に複製されると、コンテンツ提供者の利益が不当に害される。

このような問題を解決するために、個々の記録媒体を識別する ID を各記録媒
体に記録し、その ID を基に不正に複製された記録媒体を特定するシステムが知
られている。

【0003】

【発明が解決しようとする課題】

しかしながら、上述した従来のシステムでは、記録媒体に記録されたIDが改竄されたものであるか、並びに正当な権限を有する者が生成したかを検証することができないという問題がある。

【0004】

本発明は上述した従来技術の問題点に鑑みてなされ、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することを第1の目的とする。

また、本発明は、上記第1の目的を達成するデータ処理方法、そのプログラム、その装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することを第2の目的とする。

また、本発明は、上述した第1の目的を達成するデータ処理方法、そのプログラム、その装置によって生成された識別データを記録した記録媒体を提供することを第3の目的とする。

【0005】**【課題を解決するための手段】**

上述した目的を達成するために、第1の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第1の工程と、前記第1の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の工程とを有する。

【0006】

第1の発明のデータ処理方法の作用は以下のようになる。

先ず、第1の工程において、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する。

次に、第2の工程において、前記第1の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てて。

上記各工程はデータ処理装置が実行する。

【0007】

第2の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第1の手順と、前記第1の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の手順とを有する。

【0008】

第3の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第1の手段と、前記第1の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の手段とを有する。

【0009】

第3の発明のデータ処理装置の作用は以下ようになる。

まず、第1の手段が、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する。

次に、第2の手段が、前記第1の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当て第2の手段とを有する。

【0010】

第4の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程を有する。

当該工程はデータ処理装置によって実行される。

【0011】

第5の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順を有する。

【0012】

第6の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手段を有する。

【0013】

第7の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の工程と、前記第1の工程で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第2の工程とを有する。

【0014】

第7の発明のデータ処理方法の作用は以下のようになる。

先ず、第1の工程において、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する。

次に、第2の工程において、前記第1の工程で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる。

【0015】

第8の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の手順と、前記第1の手順で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第2の手順とを有する。

【0016】

第9の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する第1の手段と、前記第1の手段で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第2の手段とを有する。

【0017】

第9の発明のデータ処理装置の作用は以下になる。

まず、第1の手段が、前記識別データの管理元の秘密鍵データとデータSとを用いて、前記管理元の公開鍵データを基に前記データSを復号可能な複数の異なる署名データを生成する。

次に、第2の手段が、前記第1の手段で生成した前記複数の署名データの各々について、当該署名データと前記データSとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる。

【0018】

第10の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の工程と、前記第1の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の工程とを有する。

【0019】

第10の発明のデータ処理方法の作用は以下になる。

まず、第1の工程において、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと

前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する。

次に、第2の工程において、前記第1の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する。

上記各工程はデータ処理装置によって実行される。

【0020】

第11の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手順と、前記第1の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手順とを有する。

【0021】

第12の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成し、当該第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する第1の手段と、前記第1の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する第2の手段とを有する。

【0022】

第12の発明のデータ処理装置の作用は以下になる。

まず、第1の手段が、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第1のデータを生成する。

次に、前記第1の手段が、前記第1のデータと前記識別データ内の第2のデータとを比較して前記識別データの正当性を検証する。

次に、第2の手段が、前記第1の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第2のデータを用いて復号する。

【0023】

第13の発明のデータ処理方法は、公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 $p(w)$ の積とし、wを $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体 $STM(w)$ の各々に割当てる識別データ $ID(w)$ を生成するデータ処理方法であって、 $(K^T / p(w) \bmod M)$ を算出する第1の工程と、 $p(w)$ と前記第1の工程で算出した $(K^T / p(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てる第2の工程とを有する。

【0024】

第13の発明のデータ処理方法の作用は以下のようになる。

まず、第1の工程において、 $(K^T / p(w) \bmod M)$ を算出する。

次に、第2の工程において、 $p(w)$ と前記第1の工程で算出した $(K^T / p(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てる。

上記各工程は、データ処理装置によって実行される。

【0025】

第14の発明のプログラムは、公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 $p(w)$ の積とし、wを $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体 $STM(w)$ の各々に割当てる識別データ $ID(w)$ を生成するデータ処理装置が実行するプログラムであって、 $(K^T / p(w) \bmod M)$ を算出する第1の手順と、 $p(w)$ と前記第1の手順で算出した $(K^T / p(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てる第2の手順とを有する。

【0026】

第15の発明のデータ処理装置は、公開されたデータMを2つの素数の積とし、TをW ($W \geq 2$) 個の異なる素数 $p(w)$ の積とし、wを $1 \leq w \leq W$ の整数とし、Kを巡回群 Z^*_M の生成元とした場合に、W個の記録媒体STM(w)の各々に割当てる識別データID(w)を生成するデータ処理装置であって、 $(KT/p(w) \bmod M)$ を算出する第1の手段と、 $p(w)$ と前記第1の手段が算出した $(KT/p(w) \bmod M)$ とを含む識別データID(w)を、記録媒体STM(w)に割当てる第2の手段とを有する。

【0027】

第15の発明のデータ処理装置の作用は以下のようになる。

まず、第1の手段が、 $(KT/p(w) \bmod M)$ を算出する。

次に、第2の手段が、 $p(w)$ と前記第1の手段が算出した $(KT/p(w) \bmod M)$ とを含む識別データID(w)を、記録媒体STM(w)に割当てる。

【0028】

第16の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータpが素数であるか否かを検証する第1の工程と、前記第1の工程で前記データpが素数であると検証された場合に、前記識別データに含まれるデータIDKeyと前記データpと公開されているデータMと用いて $(IDKey p \bmod M)$ を算出する第2の工程と、前記第2の工程で算出した $(IDKey p \bmod M)$ を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の工程とを有する。

【0029】

第16の発明のデータ処理方法の作用は以下のようになる。

まず、第1の工程において、前記識別データに含まれるデータpが素数であるか否かを検証する。

次に、第2の工程において、前記第1の工程で前記データpが素数であると検証された場合に、前記識別データに含まれるデータIDKeyと前記データpと公開されているデータMと用いて $(IDKey p \bmod M)$ を算出する。

次に、第3の工程において、前記第2の工程で算出した ($IDKeyP \bmod M$) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

上記各工程は、データ処理装置によって実行される。

【0030】

第17の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータ p が素数であるか否かを検証する第1の手順と、前記第1の手順で前記データ p が素数であると検証された場合に、前記識別データに含まれるデータ $IDKey$ と前記データ p と公開されているデータ M と用いて ($IDKeyP \bmod M$) を算出する第2の手順と、前記第2の手順で算出した ($IDKeyP \bmod M$) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の手順とを有する。

【0031】

第18の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データに含まれるデータ p が素数であるか否かを検証する第1の手段と、前記第1の手段が前記データ p が素数であると検証した場合に、前記識別データに含まれるデータ $IDKey$ と前記データ p と公開されているデータ M と用いて ($IDKeyP \bmod M$) を算出する第2の手段と、前記第2の手段が算出した ($IDKeyP \bmod M$) を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第3の手段とを有する。

【0032】

第18の発明のデータ処理装置の作用は以下のようになる。

先ず、第1の手段が、前記識別データに含まれるデータ p が素数であるか否かを検証する。

次に、第2の手段が、前記第1の手段が前記データ p が素数であると検証した場合に、前記識別データに含まれるデータ $IDKey$ と前記データ p と公開されているデータ M と用いて ($IDKeyP \bmod M$) を算出する。

次に、第3の手段が、前記第2の手段が算出した $(IDKeyP \bmod M)$ を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

【0033】

第19の発明のデータ処理方法は、素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理方法であって、巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(Sd(w) \bmod M)$ を算出する第1の工程と、前記 $e(w)$ と前記第1の工程で算出した $(Sd(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てて第2の工程とを有する。

【0034】

第19の発明のデータ処理方法の作用は以下のようになる。

まず、第1の工程において、巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(Sd(w) \bmod M)$ を算出する。

次に、第2の工程において、前記 $e(w)$ と前記第1の工程で算出した $(Sd(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てて。

上記各工程は、データ処理装置によって実行される。

【0035】

第20の発明のプログラムは、素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当てて識別データ $ID(w)$ を生成するデータ処理装置が実行するプログラムであって、巡回群 Z^*_M の生成元であるデータ S と、 λ (

M) を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S d(w) \bmod M)$ を算出する第 1 の手順と、前記 $e(w)$ と前記第 1 の手順で算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当て第 2 の手順とを有する。

【0036】

第 21 の発明のデータ処理装置は、素数 q_1 と q_2 の積であり公開されたデータを M とし、 w を $1 \leq w \leq W$ の整数とし、 W ($W \geq 2$) 個の異なるデータを $e(w)$ とし、 $e(w)$ を巡回群 Z^*_M の生成元とし、 $e(w)$ と $\lambda(M)$ は互いに素であり、 $\lambda(M)$ を $(q_1 - 1)$ と $(q_2 - 1)$ との最小公倍数とした場合に、 W 個の記録媒体 $STM(w)$ の各々に割当て識別データ $ID(w)$ を生成するデータ処理装置であって、巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S d(w) \bmod M)$ を算出する第 1 の手段と、前記 $e(w)$ と前記第 1 の手段が算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当て第 2 の手段とを有する。

【0037】

第 21 の発明のデータ処理装置の作用は以下になる。

先ず、第 1 の手段が、巡回群 Z^*_M の生成元であるデータ S と、 $\lambda(M)$ を法としたときの $e(w)$ の逆数であるデータ $d(w)$ と、上記データ M とを用いて、 $(S d(w) \bmod M)$ を算出する。

次に、第 2 の手段が、前記 $e(w)$ と前記第 1 の手段が算出した $(S d(w) \bmod M)$ とを含む識別データ $ID(w)$ を、記録媒体 $STM(w)$ に割当てる。

【0038】

第 22 の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータ e およびデータ I と公開されているデータ M とを用いて $(I e \bmod M)$ を算出する第 1 の工程と、前記第 1 の工程で算出した $(I e \bmod M)$ を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第

2の工程とを有する。

【0039】

第22の発明のデータ処理方法の作用は以下になる。

先ず、第1の工程において、前記識別データに含まれるデータeおよびデータIと公開されているデータMと用いて $(I^e \bmod M)$ を算出する。

次に、第2の工程において、前記第1の工程で算出した $(I^e \bmod M)$ を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する。

【0040】

第23の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータeおよびデータIと公開されているデータMと用いて $(I^e \bmod M)$ を算出する第1の手順と、前記第1の手順で算出した $(I^e \bmod M)$ を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手順とを有する。

【0041】

第24の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データに含まれるデータeおよびデータIと公開されているデータMと用いて $(I^e \bmod M)$ を算出する第1の手段と、前記第1の手が算出した $(I^e \bmod M)$ を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第2の手段とを有する。

【0042】

第24の発明のデータ処理装置の作用は以下になる。

先ず、第1の手段が、前記識別データに含まれるデータeおよびデータIと公開されているデータMと用いて $(I^e \bmod M)$ を算出する。

次に、第2の手段が、前記第1の手が算出した $(I^e \bmod M)$ を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する。

【0043】

第25の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒

体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録している。

【0044】

第26の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒体の管理元の公開鍵データを用いて第1のデータを生成するために用いられる署名データと、前記第1のデータと比較して識別データの正当性を検証するために用いられる第2のデータとを含み前記記録媒体を識別する前記識別データを記録している。

【0045】

第27の発明の記録媒体は、暗号データを記録する記録媒体であって、素数であるデータ p と、前記暗号データを復号するために用いられるコンテンツ鍵データである($IDKeyP \bmod M$)を前記データ p と公開されているデータ M と共に算出するために用いられるデータ $IDKey$ とを含み前記記録媒体を識別する識別データを記録している。

【0046】

第28の発明の記録媒体は、暗号データを記録する記録媒体であって、前記暗号データを復号するために用いられるコンテンツ鍵データである($Ie \bmod M$)を、公開されているデータ M と共に算出するために用いられるデータ e およびデータ I とを含み前記記録媒体を識別する識別データを記録している。

【0047】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

第1実施形態

当該実施形態は、第1～第6および第25の発明に対応した実施形態である。

〔ディスク型記録媒体2〕

図1は、本発明の実施形態に係わるディスク型記録媒体2（第25の発明の記録媒体）に記録されるデータを説明するための図である。

ディスク型記録媒体2は、CD(Compact Disc)、DVD(Digital Versatile Disk)、MD(Mini Disk)やその他のディスク型の記録媒体である。

ディスク型記録媒体 2 が第 25 の発明の記録媒体に対応している。なお、本発明の記録媒体は、ディスク型以外に、フラッシュメモリなどの半導体記録装置やその他の記録媒体であってもよい。

【0048】

図 1 に示すように、ディスク型記録媒体 2 には、ディスク ID と、暗号化コンテンツデータ ECONT と、暗号鍵情報 EKB と、ディスク ID のリボケーションリスト DIRL とが記録される。

ディスク ID は、ディスク型記録媒体 2 を識別するための識別データであり、消去や書き換えが困難であるようにディスク型記録媒体 2 に格納される。

ディスク ID が本発明の識別データに対応している。ディスク ID の生成方法については後述する。

なお、以下に説明する実施形態では、ディスク状の媒体をコンテンツ格納情報記録媒体の例として示しているのので、その識別データをディスク ID として説明する。

フラッシュメモリ等の各種の情報記録媒体を利用した場合にもディスク ID に対応する識別データが設定される。

【0049】

暗号化コンテンツデータ ECONT は、暗号化されたコンテンツデータであり、暗号化コンテンツデータ ECONT を復号するためのコンテンツ鍵データは、例えば階層型鍵データ配信構成によって、正当なコンテンツ利用機器としての再生装置に提供されるデバイスノード鍵データ (DNK: Device Node Key) に基づいて、ディスク型記録媒体 2 に格納された暗号鍵情報である有効化鍵ブロック (EKB: Enabling Key Block) の復号処理等によって取得される。

階層型鍵データ配信構成によるデバイスノード鍵データ DNK の提供、およびデバイスノード鍵データ DNK に基づく有効化鍵ブロック EKB の復号処理による鍵取得処理の詳細については後述する。

【0050】

また、ディスク ID のリボケーションリスト (DIRL: Disc ID Revocation List) は、不正コピー等が行われたと認定されたディスク、例えば市場に不正な

コピーコンテンツを格納したCD-Rが発見された場合に、その不正CD-RにコンテンツとともにコピーされたディスクIDを抽出し、リスト化したデータである。リボケーションリストDIRLの生成、管理、ディスク製造者に対するリスト情報提供は、特定の信頼される管理局（CA: Central Authority）が実行する。

【0051】

〔システム構成〕

図2は、本発明の第1実施形態に係わるコンテンツ提供システム1の構成図である。

図2に示すように、コンテンツ提供システム1は、管理局CAが使用する管理装置12と、コンテンツプロバイダが使用するコンテンツ提供装置13と、ディスク製造者が使用するディスク製造装置14と、ユーザが使用する再生装置15とを有する。

ここで、管理装置12が第2および第3の発明のデータ処理装置に対応している。

また、再生装置15が第5および第6の発明のデータ処理装置に対応している。

なお、本実施形態では、再生装置15を例示するが、ディスク型記録媒体2に記録されたディスクIDの正当性を検証し、その結果を基に処理を行うのであれば、再生装置15の他に、例えば、ディスク型記録媒体2から読み出したコンテンツデータを記録または編集などを行うデータ処理装置を用いてもよい。

【0052】

管理装置12が、前述したディスクIDとリボケーションリストDIRLとを生成してディスク製造装置14に提供する。

また、コンテンツ提供装置13が、暗号化コンテンツECONTと有効化鍵ブロックEKBとをディスク製造装置14に提供する。

ディスク製造装置14は、管理装置12から受けたディスクIDおよびリボケーションリストDIRLと、コンテンツ提供装置13から受けた暗号化コンテンツデータECONTと有効化鍵ブロックEKBとを記録したディスク型記録媒体

2を製造する。

ユーザは、ディスク型記録媒体2を例えば購入し、再生装置15にセットする

。

再生装置15は、ディスク型記録媒体2に記録されたディスクIDが正当であると検証し、当該ディスクIDがリボケーションリストDIRL内に存在しないことを確認し、自らのデバイスノード鍵データDNKに基づいて有効化鍵ブロックEKBから適切なコンテンツ鍵データを取得したことを条件に、暗号化コンテンツデータECONTを復号し、続いて再生する。

【0053】

以下、図2に示すコンテンツ提供システム1を構成する各装置について詳細に説明する。

〔管理装置12〕

図3は、図2に示す管理装置12の構成図である。

図3に示すように、管理装置12は、例えば、メインメモリ22、セキュアメモリ23、入出力インタフェース(I/F)24、記録媒体インタフェース(I/F)25、演算ユニット26およびコントローラ27を有し、これらがバス21を介して接続されている。

【0054】

メインメモリ22は、演算ユニット26およびコントローラ27の処理に用いられる種々のデータのうち、セキュリティレベルが低いデータを記憶する。

セキュアメモリ23は、演算ユニット26およびコントローラ27の処理に用いられる種々のデータのうち、セキュリティレベルが高いデータを記憶する。

セキュアメモリ23は、例えば、ディスクIDの生成に用いられる管理局CAの秘密鍵データなどを記憶する。

入出力インタフェース24は、例えば、図示しない操作手段あるいはネットワークなどに接続され、管理装置12が使用する種々のデータを入力する。

記録媒体インタフェース25は、コントローラ27の制御の基に生成されたディスクIDおよびリボケーションリストDIRLを記録媒体29aに書き込む。

記録媒体29aは、コンテンツ提供装置13に提供される。

また、記録媒体インタフェース 25 は、コントローラ 27 の制御の基に生成されたデバイスノード鍵データ D N K を記録媒体 29 b に書き込む。

記録媒体 29 b は、再生装置 15、あるいは再生装置 15 の製造元に提供される。

【0055】

演算ユニット 26 は、コントローラ 27 からの制御に基づいて、署名データを生成し、これを基にディスク I D を生成する。

また、演算ユニット 26 は、リボケーションリスト D I R L を生成する。

コントローラ 27 は、プログラム P R G 1（第 2 の発明のプログラム）を実行して管理装置 12 の処理を統括的に制御する。

本実施形態における管理装置 12 の機能（処理）は、コントローラ 27 によるプログラム P R G 1 の実行に応じて規定される。

管理装置 12 の機能（処理）の全部あるいは一部は、プログラム P R G 1 によって規定されてもよいし、ハードウェアによって実現されてもよい。

【0056】

以下、図 3 に示す管理装置 12 によるディスク I D の生成動作を説明する。

図 4 は、図 3 に示す管理装置 12 によるディスク I D の生成動作を説明するためのフローチャートである。

図 4 において、ステップ S T 2 が第 1 の発明の第 1 の工程に対応し、ステップ S T 3 が第 1 の発明の第 2 の工程に対応している。

また、コントローラ 27 がステップ S T 2 を実行することで第 3 の発明の第 1 の手段が実現され、ステップ S T 3 を実行することで第 3 の発明の第 2 の手段が実現される。

【0057】

ステップ S T 1 :

管理装置 12 のコントローラ 27 は、デジタル署名のための鍵データである管理局 C A の公開鍵データ（第 1 の発明の公開鍵データ）および秘密鍵データ（第 1 ～第 3 の発明の秘密鍵データ）、並びに署名生成および検証のためのパラメータを決定する。

コントローラ 27 は、上記公開鍵データおよび上記パラメータを公開する。

コントローラ 27 は、例えば、出力インタフェース 24 からネットワーク上に上記公開鍵データおよび上記パラメータを送信して上記公開を行う。

ステップ S T 1 の処理は、管理装置 12 のセットアップ時に一度だけ行えばよい。

【0058】

ステップ S T 2 :

管理装置 12 は、入出力インタフェース 24 を介して、コンテンツプロバイダから、コンテンツ（たとえば映画）のタイトルと、製造するディスク型記録媒体 2 の枚数 W ($W \geq 2$) を入力し、これをメインメモリ 22 に格納する。

演算ユニット 26 は、任意のメッセージ M （第 1 の発明の第 2 のデータ）と、乱数 $r(w)$ と、管理局 CA の秘密鍵データとを用いて、 W 個のデジタルの異なる署名データ $SIG(w)$ （第 1 ～ 第 3 の発明の署名データ）を生成する。

当該署名データ $SIG(w)$ は、管理局 CA の上記秘密鍵データに対応する公開鍵データを用いて、その改竄の有無、並びに正当性を確認可能な形態で生成される。

ここで、 $w = 1, 2, \dots, W$ であり、 $r(w)$ はそれぞれ個別の乱数である。

なお、演算ユニット 26 は、それぞれ個別の W 個のメッセージ $M(w)$ （必ずしも個別の乱数でなくてもよい）を基に、署名データ $SIG(w)$ を生成してもよい。

演算ユニット 26 は、上記署名データ $SIG(w)$ の生成方法として、署名生成時に署名者が任意の乱数を使うことができる方法である、FIPS PUB 186-2 で米国標準の署名方式となっている DSA や、その楕円曲線暗号版である $ECDSA$ などを用いている。 DSA (Digital Signature Algorithm) はたとえば、岡本龍明、山本博資著、「現代暗号」、産業図書、1997 の pp. 179-180 に解説が記されており、 $ECDSA$ に関して <http://group.per.ieee.org/groups/1363/tradPK/index.html> から入手可能な仕様書にその詳細が記されている。

【0059】

ステップST3:

コントローラ27は、ステップST1で決定したメッセージMあるいはM(w)とステップST2で生成した署名データSIG(w)とを用いて、(M, SIG(w))の組もしくは(M(w), SIG(w))の組をw番目のディスクID(w)として生成し、それをタイトルとともにディスク製造者にセキュアな状態で提供する。

具体的には、例えば、図3に示す記録媒体29aにディスクID(w)を記録してディスク製造者に提供する。

【0060】

また、管理装置12は、リボークする情報記録媒体のディスクIDを示すリボケーションリストDIRLを生成し、これもディスク製造者に提供する。

【0061】

[ディスク製造装置14]

図5は、図1に示すディスク製造装置14の構成図である。

図5に示すように、ディスク製造装置14は、例えば、入出力インタフェース32、暗号処理部33、メモリ34、コントローラ35および記録媒体インタフェース36を有し、これらがバス31を介して接続されている。

【0062】

入出力インタフェース32は、外部から供給されるデジタル信号を受信し、バス31上に出力する。

入出力インタフェース32は、例えば、コンテンツ提供装置13からの暗号化コンテンツデータECONTおよび有効化鍵ブロックEKBを入力する。

また、入出力インタフェース32は、上記記録媒体19aなどを介して管理装置12からディスクID(w)およびリボケーションリストDIRLなどのデータを入力する。

なお、入出力インタフェース32は、製造するディスクの数に応じた数のディスクID(w)を管理装置12から受ける。

また、入出力インタフェース32は、コンテンツ提供装置13から記録媒体な

どを介して暗号化コンテンツデータ ECONT および有効化鍵ブロック EKB を入力する。

【0063】

暗号処理部 33 は、例えば、1 チップの LSI (Large Scale Integrated Circuit) で構成され、バス 31 を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス 31 上に出力する構成を持つ。

なお、暗号処理部 33 は 1 チップ LSI に限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

【0064】

メモリ 34 は、コンテンツ提供装置 13 から受領した暗号化コンテンツデータ ECONT および有効化鍵ブロック EKB と、管理装置 12 から受けたディスク ID およびリボケーションリスト DIRL とを格納する。

【0065】

コントローラ 35 は、ディスク製造装置 14 の処理を統括的に制御する。

記録媒体インタフェース 36 は、コントローラ 35 の制御の基に、種々のデータを書き込んだ図 1 に示すディスク型記録媒体 2 を製造する。

【0066】

以下、図 5 に示すディスク製造装置 14 の動作例を説明する。

図 6 は、図 5 に示すディスク製造装置 14 の動作例を説明するためのフローチャートである。

ステップ ST11:

ディスク製造装置 14 は、入出力インタフェース 32 を介して、上記記録媒体 19a を介して W 個のディスク ID (w) およびリボケーションリスト DIRL を管理装置 12 から入力してメモリ 34 に書き込む。

ステップ ST12:

ディスク製造装置 14 は、入出力インタフェース 32 を介して、有効化鍵ブロック EKB をコンテンツ提供装置 13 から入力してメモリ 34 に書き込む。

ステップ ST13:

ディスク製造装置 14 は、入出力インタフェース 32 を介して、暗号化コンテ

ンツデータ ECONT をコンテンツ提供装置 13 から入力してメモリ 34 に書き込む。

【0067】

ステップ ST14：

ディスク製造装置 14 のコントローラ 35 は、リボケーションリスト DIRL、有効化鍵ブロック EKB および暗号化コンテンツデータ ECONT をメモリ 34 から読み出し、これらのデータを情報記録媒体（ディスク）に書き込んでマスターディスクを製造する。

ステップ ST15：

コントローラ 35 は、ステップ ST14 で製造したマスターディスクに基づくスタンパによるスタンプ処理により、複製としてのディスクを製造する。

ステップ ST16：

コントローラ 35 は、ステップ ST15 で製造したディスクに、メモリ 34 から読み出したディスク ID (w) を書き込んでディスク型記録媒体 2 を製造する。

ステップ ST17：

コントローラ 35 は、W 枚のディスク型記録媒体 2 を製造したか否かを判断し、製造したと判断した場合には処理を終了し、そうでない場合にはステップ ST15 の処理に戻る。

【0068】

このように、ディスク製造装置 14 は、管理装置 12 から受けたディスク型記録媒体 2 の数 W に応じて、それぞれの製造ディスクに異なるディスク ID (w) を書き込む。

従って、市場に流通するディスク型記録媒体 2 にはそれぞれ異なるディスク ID (w) が設定されていることになり、同一のディスク ID (w) が記録された複数のディスク型記録媒体 2 が発見された場合は、不正なコピーが実行されているものと判断し、管理局 CA がリボケーションリスト DIRL にそのディスク ID (w) を書き込む更新処理を実行し、更新されたリストがディスク製造業者に提供され、新規ディスクには、そのリストが格納される。

【0069】

ディスク型記録媒体2を購入したユーザが、再生装置15にディスク型記録媒体2をセットし、コンテンツ再生処理を実行する際には、再生装置15内のメモリに格納されたりボケーションリストDIRLとのバージョン比較が実行され、更新されたりリストがメモリに格納される。従って、ユーザの再生装置15のメモリに格納されるリストは、随時更新される。

【0070】

以下、管理装置12が製造するリボケーションリストDIRLについて説明する。

図7は、図1に示すリボケーションリストDIRLを説明するための図である。

図7に示すように、リボケーションリストDIRLは、当該リボケーションリストDIRLが作成された時期に応じて値が増加するバージョン番号51と、無効に（リボーク）すべきディスク型記録媒体2のディスクID（w）を羅列したリボークディスクIDリスト52と、バージョン番号51とリボークディスクIDリスト52に対する改竄検証値53としての認証子が含まれる。

改竄検証値53は、対象となるデータ、この場合はバージョン番号51とリボークディスクIDリスト52が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード（MAC：Message Authentication Code）が適用される。

【0071】

改竄検証値53として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局CAの署名検証鍵（公開鍵）を再生機が取得し、管理局CAの署名生成鍵（秘密鍵）を用いて作られた署名を各再生機が取得した署名検証鍵（公開鍵）によって検証することで、バージョン番号51とリボークディスクIDリスト52が改竄されているか否かを判別する。

【0072】

図8は、改竄検証値53としてメッセージ認証コードMACを用いた際のMA

C生成、検証処理を説明するための図である。

メッセージ認証コードMACは、データの改竄検証用のデータとして生成されるものであり、MAC生成処理、検証処理態様には様々な態様が可能であるが、1例としてDES暗号処理構成を用いたMAC値生成例を図8を基に説明する。

【0073】

図8に示すように、対象となるメッセージ、この場合は、図7に示すバージョン番号51とリボークディスクIDリスト52を8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、・・・、MNとする)、まず、初期値(Initial Value (IV))とM1を排他的論理和する(その結果をI1とする)

。

次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。

続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号MACとなる。

【0074】

MAC値は、その生成元データが変更されると、異なる値となり、検証対象のデータ(メッセージ)に基づいて生成したMACと、記録されているMACとの比較を行い、一致していれば、検証対象のデータ(メッセージ)は変更、改竄がなされていないことが証明される。

【0075】

MAC生成における鍵K1としては、たとえば、階層型鍵データ配信構成によるデバイスノード鍵データDNKに基づく有効化鍵ブロック(EKB)の復号処理によって得られる鍵(ルート鍵データ)を適用することが可能である。また、初期値IVとしては、予め定めた値を用いることが可能である。

【0076】

〔階層型鍵配信ツリー構成〕

以下、ブロードキャストエンクリプション(Broadcast Encryption)方式の一

態様である階層型鍵配信ツリー構成に従った鍵提供処理、再生機としての再生装置管理構成について説明する。

【0077】

図9の最下段に示すナンバ0～15がコンテンツ利用を行なうユーザデバイスである。本実施形態では、当該ユーザデバイスは、図2に示す再生装置15に対応している。

図4に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

【0078】

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図9に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノード鍵データ）および各リーフのリーフ鍵データからなる鍵データセット（デバイスノード鍵データDNKをメモリに格納する。

図9の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフ鍵データであり、最上段のKR（ルート鍵データ）から、最下段から2番目の節（ノード）に記載された鍵データ：KR～K111をノード鍵データとする。

【0079】

図9に示すツリー構成において、例えばデバイス0はリーフ鍵データK0000と、ノード鍵データ：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。

なお、図9のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0080】

また、図9のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、

MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。

さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図9に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0081】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図9の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いる1つのグループとして設定する。

例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはCD等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵データを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。

コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティティは、図9の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図9のツリー中に複数存在する。

【0082】

なお、ノード鍵データ、リーフ鍵データは、ある1つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノード鍵データ、リーフ鍵データは例えば鍵データの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

【0083】

このツリー構造において、図9から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はデバイスノード鍵データDNKとして共通の

鍵データK00、K0、KRを含むデバイスノード鍵データDNKを保有する。

このノード鍵データ共有構成を利用することにより、例えば共通の鍵データをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノード鍵データK00は、デバイス0、1、2、3に共通する保有鍵データとなる。

また、新たな鍵データKnewをノード鍵データK00で暗号化した値Enc(K00, Knew)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノード鍵データK00を用いて暗号Enc(K00, Knew)を解いて新たな鍵データKnewを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0084】

また、ある時点tにおいて、デバイス3の所有する鍵：K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0、1、2、3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。

そのためには、ノード鍵データ：K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0、1、2にその更新鍵データを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新鍵データであることを示す。

【0085】

更新鍵データの配布処理について説明する。鍵データの更新は、例えば、図10（A）に示す有効化鍵ブロックEKBによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0、1、2に供給することによって実行される。

なお、有効化鍵ブロックEKBは、図9に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新された鍵データを配布するための暗号化鍵データによって構成される。有効化鍵ブロックEKBは、鍵データ更新ブロッ

ク (KRB: Key Renewal Block) と呼ばれることもある。

【0086】

図10 (A) に示す有効化鍵ブロック EKB には、ノード鍵データの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。

図10の例は、図9に示すツリー構造中のデバイス0, 1, 2において、世代 t の更新ノード鍵データを配布することを目的として形成されたブロックデータである。

図9から明らかなように、デバイス0, デバイス1は、更新ノード鍵データとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノード鍵データとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

【0087】

図10 (A) の EKB に示されるように EKB には複数の暗号化鍵データが含まれる。最下段の暗号化鍵データは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフ鍵データ $K0010$ によって暗号化された更新ノード鍵データ $K(t)001$ であり、デバイス2は、自身の持つリーフ鍵データによってこの暗号化鍵データを復号し、 $K(t)001$ を得ることができる。

また、復号により得た $K(t)001$ を用いて、図10 (A) の下から2段目の暗号化鍵データ $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノード鍵データ $K(t)00$ を得ることができる。

以下順次、図10 (A) の上から2段目の暗号化鍵データ $Enc(K(t)00, K(t)0)$ を復号し、更新ノード鍵データ $K(t)0$ 、図10 (A) の上から1段目の暗号化鍵データ $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノード鍵データ $K000$ は更新する対象に含まれておらず、更新ノード鍵データとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。

デバイス $K0000$ 、 $K0001$ は、図10 (A) の上から3段目の暗号化鍵

データ $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図10(A)の上から2段目の暗号化鍵データ $Enc(K(t)00, K(t)0)$ を復号し、更新ノード鍵データ $K(t)0$ 、図10(A)の上から1段目の暗号化鍵データ $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0, 1, 2は更新した鍵 $K(t)R$ を得ることができる。

なお、図10(A)のインデックスは、復号鍵データとして使用するノード鍵データ、リーフ鍵データの絶対番地を示す。

【0088】

図9に示すツリー構造の上位段のノード鍵データ: $K(t)0, K(t)R$ の更新が不要であり、ノード鍵データ $K00$ のみの更新処理が必要である場合には、図10(B)の有効化鍵ブロック EKB を用いることで、更新ノード鍵データ $K(t)00$ をデバイス0, 1, 2に配布することができる。

【0089】

図10(B)に示す EKB は、例えば特定のグループにおいて共有する新たなコンテンツ鍵データを配布する場合に利用可能である。

具体例として、図9に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツ鍵データ $K(t)con$ が必要であるとする。

このとき、デバイス0, 1, 2, 3の共通のノード鍵データ $K00$ を更新した $K(t)00$ を用いて新たな共通の更新コンテンツ鍵データ: $K(t)con$ を暗号化したデータ $Enc(K(t)00, K(t)con)$ を図10(B)に示す EKB とともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0090】

すなわち、デバイス0, 1, 2は EKB を処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データ $K(t)con$ を得ることが可能になる。

【0091】

図11に、 t 時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データ $K(t)_{con}$ をEKBの処理によって取得する処理例を示す。

EKBには、 $K(t)_{00}$ を用いてコンテンツ鍵データ $K(t)_{con}$ を暗号化したデータ $Enc(K(t)_{00}, K(t)_{con})$ と図10(B)に示すデータとが格納されているとする。ここでは、デバイス0の処理例を示す。

【0092】

図11に示すように、デバイス0は、記録媒体に格納されている世代： t 時点のEKBと自分があらかじめ格納しているノード鍵データ $K000$ を用いて上述したと同様のEKB処理により、ノード鍵データ $K(t)_{00}$ を生成する。

さらに、復号した更新ノード鍵データ $K(t)_{00}$ を用いて暗号化データ $Enc(K(t)_{00}, K(t)_{con})$ を復号して更新コンテンツ鍵データ $K(t)_{con}$ を取得する。さらに、デバイスは、後にそれを使用するために自分だけが持つリーフ鍵データ $K0000$ で暗号化して格納してもよい。

【0093】

また、別の例として、ツリー構造のノード鍵データの更新は不必要で、時点 t でのコンテンツ鍵データ $K(t)_{con}$ のみを必要な機器が得られればよい、という場合もある。この場合、下記のような方式とすることができる。

【0094】

いま、図11の例と同様に、デバイス0、1、2にのみコンテンツ鍵データ $K(t)_{con}$ を送りたいとする。このとき、EKBは、

バージョン (Version) : t

インデックス 暗号化鍵データ

000 $Enc(K000, K(t)_{con})$

0010 $Enc(K0010, K(t)_{con})$

となる。

【0095】

デバイス0、1は $K000$ を用いて、またデバイス2は $K0010$ を用いて上記EKBのうちの1つの暗号文を復号することによりコンテンツ鍵データを得る

ことができる。このようにすることにより、ノード鍵データの更新は行えないものの、必要な機器にコンテンツ鍵データを与える方法をより効率よく（すなわち、EKBに含まれる暗号文数を減らしてEKBのサイズを小さくするとともに、管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

【0096】

図12に有効化鍵ブロックEKBのフォーマット例を示す。バージョン61は、有効化鍵ブロックEKBのバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化鍵ブロックEKBの配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ63は、有効化鍵ブロックEKB中のデータ部の位置を示すポインタであり、タグポインタ64はタグ部の位置、署名ポインタ65は署名の位置を示すポインタである。

【0097】

データ部66は、例えば更新するノード鍵データを暗号化したデータを格納する。例えば図5に示すような更新されたノード鍵データに関する各暗号化鍵データ等を格納する。

【0098】

タグ部67は、データ部に格納された暗号化されたノード鍵データ、リーフ鍵データの位置関係を示すタグである。このタグの付与ルールを図13を用いて説明する。

図13では、データとして先に図10(A)で説明した有効化鍵ブロックEKBを送付する例を示している。

この時のデータは、図13の表(b)に示すようになる。このときの暗号化鍵データに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルート鍵データの更新鍵データ $K(t)R$ が含まれているので、トップノードアドレスは KR となる。

このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図13の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、 Enc

(K(t) 00, K(t) 0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは {左(L) タグ, 右(R) タグ} として設定される。最上段のデータ Enc(K(t) 0, K(t) R) の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図13(c) に示すデータ列、およびタグ列が構成される。

【0099】

タグは、データ Enc(Kxxx, Kyyy) がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納される鍵データ Enc(Kxxx, Kyyy) . . . は、単純に暗号化された鍵データの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化鍵データのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図10で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : Enc(K(t) 0, K(t) root)

00 : Enc(K(t) 00, K(t) 0)

000 : Enc(K((t) 000, K(T) 00)

. . . のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。

これに対し、上述したタグを鍵データ位置を示す索引データとして用いることにより、少ないデータ量で鍵データ位置の判別が可能となる。

【0100】

図12に戻って、EKBフォーマットについてさらに説明する。署名 (Signature) 68は、有効化鍵ブロックEKBを発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化鍵ブロックEKB発行者が発行した有効化鍵ブロックEKBであることを確認する。

【0101】

ノード鍵データ等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的な鍵データ更新処理、暗号化鍵データ配信、データ配信を実行する構成について、以下説明する。

【0102】

図14は、階層ツリー構造のカテゴリの分類の一例を説明するための図である。

図14において、階層ツリー構造の最上段には、ルート鍵データ $K_{root}71$ が設定され、以下の中間段にはノード鍵データ72が設定され、最下段には、リーフ鍵データ73が設定される。各デバイスは個々のリーフ鍵データと、リーフ鍵データからルート鍵データに至る一連のノード鍵データ、ルート鍵データを保有する。

【0103】

ここで、一例として最上段から第M段目のあるノードをカテゴリノード74として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【0104】

例えば図14の第M段目の1つのノード75にはカテゴリAが設定され、このノード以下に連なるノード、リーフはカテゴリAに区分され、様々なデバイスを含むカテゴリA専用のノードまたはリーフとして設定される。すなわち、ノード75以下を、カテゴリAとして区分されるデバイスの関連ノード、およびリーフの集合として定義する。

【0105】

さらに、M段から数段分下位の段をサブカテゴリノード76として設定することができる。

例えば図に示すようにカテゴリAノード75の2段下のノードに、カテゴリAに含まれるサブカテゴリAaノードとして、[再生専用器]のノードを設定する

さらに、サブカテゴリ A a ノードである再生専用器のノード 76 以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード 77 が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる [PHS] ノード 78 と [携帯電話] ノード 79 を設定することができる。

【0106】

さらに、カテゴリ、サブカテゴリは、デバイスの種類、メーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位で設定可能である。例えば 1 つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器 X Y Z 専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器 X Y Z にその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを格納して販売することが可能となり、その後、暗号化コンテンツデータの配信、あるいは各種鍵データの配信、更新処理を、その頂点ノード鍵データ以下のノード鍵データ、リーフ鍵データによって構成される有効化鍵ブロック E K B を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0107】

また、コンテンツプロバイダの管理するノードをカテゴリノードとした場合には、コンテンツプロバイダが提供するコンテンツを格納した C D、M D、D V D 等の情報記録媒体またはネット配信コンテンツを利用する機器をカテゴリノード以下に設定して、その機器に対してその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを提供することが可能となる。

【0108】

このように、1 つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の 1 つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化鍵ブロック (E K B) を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイ

スには全く影響を及ぼさずに鍵データ更新を実行することができる。

【0109】

例えば、図15に示されるように、ツリー構成のシステムで、鍵データ管理が行われる。

図15の例では、 $8 + 2^4 + 3^2$ 段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばフラッシュメモリなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【0110】

すなわち、このTシステムのノードよりさらに下の階層の 2^4 段のノードに対応する鍵データが、ショップサーバ、ライセンスサーバ等の管理エンティティとしてのサービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。

この例の場合、これにより、 2^{24} （約16メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の 3^2 段の階層により、 2^{32} （約4ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。

最下段の 3^2 段のノードからTシステムのノードまでのパス上の各ノードに対応する鍵データが、DNKを構成し、最下段のリーフに対応するIDがリーフIDとされる。

【0111】

例えば、コンテンツを暗号化したコンテンツ鍵データは更新されたルート鍵データKR'によって暗号化され、上位の階層の更新ノード鍵データは、その直近の下位の階層の更新ノード鍵データを用いて暗号化され、EKB内に配置される。EKBにおける末端から1つ上の段の更新ノード鍵データはEKBの末端のノード鍵データあるいはリーフ鍵データによって暗号化され、EKB内に配置される。

【0112】

ユーザデバイスは、サービスデータに記述されているDNKのいずれかの鍵データを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層の更新ノード鍵データを復号し、復号して得た鍵データを用いて、EKB内に記述されているさらにその上の階層の更新ノード鍵データを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルート鍵データKR'を得ることができる。

【0113】

上述したように、ツリーのカテゴリ分類により、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化鍵ブロックEKBを独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

【0114】

〔再生装置15〕

図16は、図2に示す再生装置15の構成図である。

図16に示すように、再生装置15は、例えば、入出力インタフェース81、MP E G (Moving Picture Experts Group)等の各種符号化データの生成および復号を実行するコーデック82、A/D・D/Aコンバータ84を備えた入出力インタフェース83、暗号処理部85、ROM (Read Only Memory) 86、コントローラ87、メモリ88、並びにディスク型記録媒体2にアクセスするための記録媒体インタフェース89を有し、これらがバス80によって相互に接続されている。

【0115】

入出力インタフェース81は、ネットワーク等、外部から供給されるデジタル信号を受信し、バス80上に出力するとともに、バス80上のデジタル信号を受信し、外部に出力する。

コーデック82は、バス80を介して供給される例えばMP E G符号化された

データをデコードし、入出力インタフェース 83 に出力するとともに、入出力インタフェース 83 から供給されるデジタル信号をエンコードしてバス 80 上に出力量する。

入出力インタフェース 83 は、コンバータ 84 を内蔵している。

入出力インタフェース 83 は、外部から供給されるアナログ信号を受信し、コンバータ 84 で A/D (Analog Digital) 変換することで、デジタル信号として、コーデック 82 に出力するとともに、コーデック 82 からのデジタル信号をコンバータ 84 で D/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0116】

暗号処理部 85 は、例えば、1 チップの L S I で構成され、バス 80 を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス 80 上に出力量する構成を持つ。

なお、暗号処理部 85 は 1 チップ L S I に限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

【0117】

R O M 86 は、例えば、再生装置ごとに固有の、あるいは複数の再生装置のグループごとに固有のデバイス鍵データであるリーフ鍵データと、複数の再生装置、あるいは複数のグループに共有のデバイス鍵データであるノード鍵データを記憶している。

コントローラ 87 は、メモリ 88 に記憶されたプログラム P R G 3 (第 5 の発明のプログラム) を実行することで、再生装置 15 の処理を統括して制御する。

すなわち、再生装置 15 の機能 (処理) は、プログラム P R G 3 によって規定される。なお、再生装置 15 の機能の全部あるいは一部を、ハードウェアによって実現してもよい。

【0118】

メモリ 88 は、上述したリボケーションリスト D I R L をディスク型記録媒体 2 から読み取りセキュアな状態で格納する。

例えば再生装置 15 に設定された I D に基づく暗号化を施してメモリに格納す

るなどにより耐タンパ性を保持したデータとして格納することが好ましい。このようにリボケーションリスト D I R L は外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。

記録媒体インタフェース 89 は、ディスク型記録媒体 2 にアクセスするために用いられる。

【0119】

以下、図 16 に示す再生装置 15 の動作例を説明する。

図 17 は図 16 に示す再生装置 15 の全体動作例を説明するためのフローチャート、図 18 は図 17 に示すステップ S T 3 2 のディスク I D の検証処理を説明するためのフローチャート、図 19 は図 17 に示すステップ S T 3 8 のコンテンツ再生を説明するためのフローチャートである。

ステップ S T 3 1 :

再生装置 15 は、所定のアクセス位置にディスク型記録媒体 2 がセットされると、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 からディスク I D を読み出し、これをメモリ 88 に格納する。

ステップ S T 3 2 :

再生装置 15 のコントローラ 87 は、ステップ S T 3 1 でメモリ 88 に格納したディスク I D を読み出してその改竄の有無および正当性を検証する。

当該検証については、後に詳細に説明する。

ステップ S T 3 3 :

コントローラ 87 は、ステップ S T 3 2 で上記ディスク I D が正当であると検証するとステップ S T 3 5 の処理に進み、そうでない場合にはステップ S T 3 4 に進む。

【0120】

ステップ S T 3 4 :

コントローラ 87 は、ディスク型記録媒体 2 に記録されている暗号化コンテンツデータ E C O N T の復号および再生を停止（禁止）する。

ステップ S T 3 5 :

コントローラ 87 は、記録媒体インタフェース 89 を介して、ディスク型記録媒体 2 からリボケーションリスト D I R L を読み出す。

そして、コントローラ 87 は、当該読み出したリボケーションリスト D I R L の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コード M A C が付与されている場合は、先に図 8 を参照して説明した M A C 検証処理が実行される。

そして、コントローラ 87 は、リボケーションリスト D I R L に改竄がないと判定されたことを条件に、当該リボケーションリスト D I R L のバージョンと、メモリ 88 に既に格納されているリボケーションリスト D I R L とのバージョン比較を実行する。

コントローラ 87 は、当該読み出したリボケーションリスト D I R L のバージョンがメモリ 88 に既に格納されているリボケーションリスト D I R L より新しい場合は、当該読み出したリボケーションリスト D I R L によって、メモリ 88 内のリボケーションリスト D I R L を更新する。

【0121】

ステップ S T 3 6 :

コントローラ 87 は、ステップ S T 3 1 で読み出したディスク I D がリボケーションリスト D I R L 内に存在するか否かを判断し、存在すると判断するとステップ S T 3 8 に進み、そうでない場合にはステップ S T 3 7 に進む。

ステップ S T 3 7 :

コントローラ 87 は、ディスク型記録媒体 2 に記録されている暗号化コンテンツデータ E C O N T の復号および再生を停止（禁止）する。

ステップ S T 3 8 :

コントローラ 87 は、ディスク型記録媒体 2 に記録されている暗号化コンテンツデータ E C O N T を読み出し、これを復号して再生する。

ステップ S T 3 8 の処理については、後に詳細に説明する。

【0122】

以下、図 17 に示すディスク I D の検証（S T 3 2）について詳細に説明する

。

図18は、図17に示すステップST32を説明するためのフローチャートである。

図18の処理が、第4の発明の工程に対応し、ステップST42が第1の工程に対応し、ステップST43～ST46が第2の工程に対応している。

また、図18の処理をコントローラ87が行うことで、第6の発明の手段が実現される。

ステップST41:

再生装置15のコントローラ87は、図17に示すステップST31で読み出したディスクID(w)内の署名データSIG(w)(第4～第6の発明の署名データ)を取り出す。

ステップST42:

コントローラ87は、メモリ88から読み出した管理装置12(管理局CA)の公開鍵データ(第4～第6の発明の公開鍵データ)および公開されたパラメータを基に、ステップST41で読み出した署名データSIG(w)からメッセージM(w)'(第4の発明の第1のデータ)を生成する。

ステップST43:

コントローラ87は、ディスクID(w)内のメッセージM(w)あるいはM(第4の発明の第2のデータ)と、ステップST42で生成したメッセージM(w)'とを比較する。

【0123】

ステップST44:

コントローラ87は、ステップST43の比較で一致していると判定するとステップST45に進み、そうでない場合にはステップST46に進む。

ステップST45:

コントローラ87は、ステップST41で取り出したディスクID(w)が正当であると判定する。

ステップST46:

コントローラ87は、ステップST41で取り出したディスクID(w)が不

正であると判定する。

【0124】

以下、図17に示すステップST38の再生処理について説明する。

図19は、図17に示すステップST38の再生処理を説明するためのフローチャートである。

ステップST51：

再生装置15は、記録媒体インタフェース89を介して、ディスク型記録媒体2から暗号鍵情報、すなわち有効化鍵ブロックEKBを読み出す。

ステップST52：

コントローラ87は、図11を用いて前述したように、階層型鍵データ配信構成によって予め再生装置に提供されているデバイスノード鍵データDNKに基づいて有効化鍵ブロックEKBの復号処理を実行して、コンテンツ鍵データを取得する。

【0125】

ステップST53：

コントローラ87は、記録媒体インタフェース89を介して、ディスク型記録媒体2から暗号化コンテンツデータECONTを読み出す。

ステップST54：

コントローラ87は、ステップST52で取得したコンテンツ鍵データを用いて、ステップST53で読み出した暗号化コンテンツデータECONTを復号する。

ステップST55：

コントローラ87は、ディスク型記録媒体2に記録されている全ての暗号化コンテンツデータECONTを復号したと判断すると、処理を終了し、そうでない場合にはステップST53に戻る。

【0126】

以上説明したように、コンテンツ提供システム1では、ディスク型記録媒体2に記録するディスクIDを、管理装置12において、管理装置12の秘密鍵データを基に署名データとして生成する。

また、再生装置 15 において、ディスク型記録媒体 2 から読み出したディスク ID を、管理装置 12 の公開鍵データを用いて検証する。

そのため、ディスク型記録媒体 2 に記録されてるディスク ID が改竄されたり、不正者によって生成された場合に、そのことを再生装置 15 などが容易に検出できる。

その結果、不正に複製されたディスク型記録媒体 2 の流通を効果的に抑制することが可能になり、コンテンツ提供者の利益を保護できる。

【0127】

上述したように、第 1 実施形態では、ディスク ID は任意の値ではなく、信頼できる機関である管理局 CA の管理装置 12 が生成し、署名したものをを用いた。

また、上述した第 1 実施形態では、コンテンツデータを暗号化して暗号化コンテンツデータ ECONT を得るために用いたコンテンツ鍵データは、ディスク ID とは独立して生成されている。

以下に示す実施形態では、コンテンツ鍵データをディスク ID から導出する場合を例示する。

これにより、不正者が、任意のディスク ID を用いて海賊版ディスクを無制限に製造する効果をさらに高めることができる。

【0128】

第 2 実施形態

第 2 実施形態は、第 7 ～ 第 12 および第 26 の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図 4 に示す管理装置 12 によるディスク ID の生成処理、図 18 に示すディスク ID の検証処理、図 19 に再生処理におけるコンテンツ復号データの取得処理を除いて、第 1 実施形態のコンテンツ提供システム 1 と同じである。

本実施形態では、ディスク ID はディスク ID からタイトルごとに共通のメッセージ S を導出できるように生成され、このメッセージ S をコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置 12 a のディスク ID 生成方法を説明する

図20は、本実施形態のコンテンツ提供システムにおいて管理装置12aが行うディスクIDの生成方法を説明するためのフローチャートである。

図20に示す各処理は、コントローラ27がプログラムPRG1aを実行することによって実現され、この場合にプログラムPRG1aが第8の発明に対応する。

また、コントローラ27が図20に示す各ステップを実行することで、第9の発明の第1の手段および第2の手段が実現される。この場合に、管理装置12aが第8および第9の発明のデータ処理装置に対応している。

なお、図20に示す処理の全部または一部は、コントローラ27がプログラムPRG1aを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

【0129】

ステップST101：

管理装置12aのコントローラ27は、デジタル署名のための鍵データ（管理局CAの公開鍵データおよび秘密鍵データ）、並びに署名生成および検証のためのパラメータを決定する。

コントローラ27は、上記公開鍵データおよび上記パラメータを公開する。

当該公開は、例えば、コントローラ27が、入出力インタフェース24を介してネットワークを介して送信を行って実現する。

ステップST101の処理は、管理装置12のセットアップ時に一度だけ行えばよい。

【0130】

ステップST102：

管理装置12は、入出力インタフェース24を介して、コンテンツプロバイダから、コンテンツ（たとえば映画）のタイトルと、製造するディスクの枚数 W （ $W \geq 2$ ）を入力し、これをメインメモリ22に格納する。

演算ユニット26は、コンテンツデータのタイトルに対してメッセージ S （第7～第9の発明のデータ S ）を決定する。

当該メッセージ S が後述する、ディスク ID から導出される値となり、コンテンツ鍵データとして用いられる。

【0131】

ステップ ST103:

演算ユニット 26 は、ステップ ST102 で決定したメッセージ S と、乱数 $r(w)$ と、上記パラメータとを用いて、W 個のデジタルの異なる署名データ SIG(w) を生成する。

ここで、 $w=1, 2, \dots, W$ であり、 $r(w)$ はそれぞれ個別の乱数である。

ステップ ST104:

コントローラ 27 は、 w 番目のディスク ID (w) として、($S, SIG(w)$) の組をタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置 14 は、図 6 を用いて前述した手順で、上記ディスク ID (w) を記録したディスク型記録媒体 2a (第 26 の発明の記録媒体) を製造する。

また、ディスク製造装置 14 は、ステップ ST102 で決定したメッセージ S を、コンテンツ鍵データとしてコンテンツデータを暗号化した暗号化コンテンツデータ ECONT をディスク型記録媒体 2a に記録する。

【0132】

以下、本実施形態における再生装置 15a の動作例を説明する。

本実施形態の再生装置 15a は、図 17 に示すステップ ST32 およびステップ ST38 の処理のみが第 1 実施形態の場合と異なる。

図 21 は、本実施形態における再生装置 15a によるディスク ID の検証を説明するためのフローチャートである。

図 21 に示す処理が第 10 の発明の第 1 の工程に対応し、図 22 に示す処理が第 10 の発明の第 2 の工程に対応している。

また、コントローラ 87 が図 21 に示す処理を実行することで第 12 の発明の第 1 の手段が実現され、図 22 の処理を実行することで第 12 の発明の第 2 の手段が実現される。

また、以下に示す処理は、再生装置 15 b のコントローラ 87 がプログラム P R G 3 c (第 17 の発明のプログラム) を実行して実現される。

【0133】

ステップ S T 1 1 1 :

再生装置 15 a のコントローラ 87 は、図 17 に示すステップ S T 3 1 で上述したディスク型記録媒体 2 a から読み出したディスク I D (w) 内の署名データ S I G (w) を取り出す。

ステップ S T 1 1 2 :

コントローラ 87 は、メモリ 88 から読み出した管理装置 12 (管理局 C A) の公開鍵データと公開されたパラメータとを基に、ステップ S T 1 1 1 で取り出した署名データ S I G (w) からメッセージ S' (第 10 ~ 第 12 の発明の第 1 のデータ) を生成する。

ステップ S T 1 1 3 :

コントローラ 87 は、ディスク I D (w) 内のメッセージ S (第 10 ~ 第 12 の発明の第 2 のデータ) と、ステップ S T 1 1 2 で生成したメッセージ S' とを比較する。

【0134】

ステップ S T 1 1 4 :

コントローラ 87 は、ステップ S T 1 1 3 の比較で一致していると判定するとステップ S T 1 1 5 に進み、そうでない場合にはステップ S T 1 1 6 に進む。

ステップ S T 1 1 5 :

コントローラ 87 は、ステップ S T 1 1 1 で取り出したディスク I D (w) が正当であると判定する。

ステップ S T 1 1 6 :

コントローラ 87 は、ステップ S T 1 1 1 で取り出したディスク I D (w) が不正であると判定する。

【0135】

図 22 は、本実施形態における図 17 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

本実施形態において、ステップ S T 5 1 が無く、ステップ S T 5 2 の代わりにステップ S T 5 2 a を行うこと以外は、図 1 9 を用いて第 1 実施形態で説明したものと同一である。

ステップ S T 5 2 a :

再生装置 1 5 a のコントローラ 8 7 は、図 2 1 の検証でディスク I D の正当性が認められたことを条件に、ディスク I D (w) 内のメッセージ S と再生装置 1 5 a が取得した図 9 を用いて説明したルート鍵データとを基にコンテンツ鍵データ (復号鍵) を生成する。コントローラ 8 7 は、例えば、ルート鍵データと、メッセージ S との排他的論理和をコンテンツ鍵データとする。

本実施形態のコンテンツ提供システムによっても、第 1 実施形態のコンテンツ提供システム 1 と同様の効果が得られる。

【0136】

第3実施形態

第3実施形態は、第 1 3 ~ 第 1 8 および第 2 7 の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図 4 に示す管理装置 1 2 によるディスク I D の生成処理、図 1 8 に示すディスク I D の検証処理、図 1 9 に再生処理におけるコンテンツ復号データの取得処理を除いて、第 1 実施形態のコンテンツ提供システム 1 と同一である。

本実施形態では、ディスク I D はディスク I D からタイトルごとに共通のメッセージ S を導出できるように生成され、このメッセージ S をコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置 1 2 b のディスク I D 生成方法を説明する。

図 2 3 は、本実施形態のコンテンツ提供システムにおいて管理装置 1 2 b が行うディスク I D の生成方法を説明するためのフローチャートである。

図 2 3 に示す各処理は、管理装置 1 2 b のコントローラ 2 7 がプログラム P R G 1 b を実行することによって実現され、この場合にプログラム P R G 1 b が第 1 4 の発明に対応する。

また、コントローラ 2 7 が図 2 3 に示す各ステップを実行することで、第 1 5 の発明の第 1 の手段および第 2 の手段が実現される。この場合に、管理装置 1 2 b が第 1 4 および第 1 5 の発明のデータ処理装置に対応している。

なお、図 2 3 に示す処理の全部または一部は、コントローラ 2 7 がプログラム P R G 1 b を実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

【0 1 3 7】

ステップ S T 2 0 1 :

管理装置 1 2 b のコントローラ 2 7 が、R S A 暗号に用いるのに安全とされる程度に大きな素数 q_1 , q_2 を選択する。

ステップ S T 2 0 2 :

コントローラ 2 7 が、ステップ S T 2 0 1 で選択した素数 q_1 , q_2 の積であるデータ M を公開する。

ステップ S T 2 0 1, S T 2 0 2 の処理はシステムのセットアップ時に一度だけ行えばよい。

【0 1 3 8】

ステップ S T 2 0 3 :

コントローラ 2 7 が、各タイトルに対して、 $K \in Z^*_M$ (K は巡回群 Z^*_M の生成元) を満たすデータ K をランダムに選択する。

ここで、例えば、 $X \in Z^*_M$ は、 X が、 $1 \sim X-1$ の整数 x のなかで x を法として逆元を持つ集合の要素であることを示す。

ステップ S T 2 0 4 :

コントローラ 2 7 が、コンテンツ製作者から、コンテンツのタイトルと製造するディスク型記録媒体 2 b 予定最大生産枚数 W を受け取る。

ステップ S T 2 0 5 :

コントローラ 2 7 が、ステップ S T 2 0 4 の枚数 W に対応した数だけ、素数 $p(w)$ ($w=1, 2, \dots, W$) を定める。例えば、 w 番目の奇素数を $p(w)$ と定めてもよい。

【0 1 3 9】

ステップST206:

コントローラ27が、そのタイトルに対応して、ディスクIDから導出される値として、データS ($=K^T \bmod M$) を決定する。

但し、下記式(1) が成り立つ。

【0140】

【数1】

$$T = \prod_{w=1}^w p_w \quad \dots (1)$$

【0141】

ステップST207:

コントローラ27が、 $(K^T/p(w) \bmod M)$ を演算して、その結果であるデータIDkey (w) を得る。

【0142】

ステップST208:

コントローラ27は、w番目のディスクID (w) として、ステップST205で決定した素数p (w) と、ステップST207で得たデータIDkey (w) との組 (p (w), IDkey (w)) をディスクIDとしてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置14は、図6を用いて前述した手順で、上記ディスクID (w) を記録したディスク型記録媒体2b (第27の発明の記録媒体) を製造する。

また、ディスク製造装置14は、上述したステップST206で決定したデータS ($=K^T \bmod M$) をコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータECONTを生成し、これをディスク型記録媒体2bに記録する。

【0143】

以下、本実施形態における再生装置15bの動作例を説明する。

本実施形態の再生装置15bは、図17に示すステップST32およびステップST38の処理のみが第1実施形態の場合と異なる。

図 24 は、本実施形態における再生装置 15b によるディスク ID の検証を説明するためのフローチャートである。

図 24 に示す処理が第 16 の発明の第 1 の工程に対応している。

また、コントローラ 87 が図 24 に示す処理を実行することで第 18 の発明の第 1 の手段が実現される。

また、以下に示す処理は、再生装置 15b のコントローラ 87 がプログラム P RG3b (第 17 の発明のプログラム) を実行して実現される。

【0144】

ステップ ST211:

再生装置 15b のコントローラ 87 は、図 17 に示すステップ ST31 で上述したディスク型記録媒体 2a から読み出したディスク ID (w) 内のデータ p (w) を取り出す。

ステップ ST212:

コントローラ 87 は、ステップ ST111 で取り出したデータ p (w) が素数か否かを判断する

コントローラ 87 は、データ p (w) が素数であると判断するとステップ ST213 に進み、そうでない場合にはステップ ST214 に進む。

ステップ ST213:

コントローラ 87 は、ステップ ST211 で取り出したディスク ID (w) が正当であると判定する。

ステップ ST214:

コントローラ 87 は、ステップ ST211 で取り出したディスク ID (w) が不正であると判定する。

【0145】

図 25 は、本実施形態における図 17 に示すステップ ST38 の再生処理を説明するためのフローチャートである。

図 25 に示すステップ ST221 が第 16 の発明の第 2 の工程に対応し、ステップ ST224 が第 16 の発明の第 3 の工程に対応する。

また、コントローラ 87 がステップ ST221 を実行することで第 18 の発明

の第1の手段が実現され、ステップST224を実行することで第18の発明の第2の手段が実現される。

ステップST221:

再生装置15bのコントローラ87は、記録媒体インタフェース89を介して、ディスク型記録媒体2から読み出したデータp, IDKeyおよび公開されているデータMを基に、(IDkeyP mod M)を算出し、その結果をデータS'とする。

ステップST222:

コントローラ87は、ステップST221で算出したデータS'と、再生装置15bが取得した図9を用いて説明したルート鍵データとを基にコンテンツ鍵データ(復号鍵)を生成する。コントローラ87は、例えば、ルート鍵データと、データS'との排他的論理和をコンテンツ鍵データとする。

ステップST223:

コントローラ87は、記録媒体インタフェース89を介して、ディスク型記録媒体2bから暗号化コンテンツデータECONTを読み出す。

ステップST224:

コントローラ87は、ステップST222のコンテンツ鍵データを用いて、ステップST223で読み出した暗号化コンテンツデータECONTを復号する。

ステップST225:

コントローラ87は、ディスク型記録媒体2bに記録されている全ての暗号化コンテンツデータECONTを復号したと判断すると、処理を終了し、そうでない場合にはステップST223に戻る。

【0146】

本実施形態のコンテンツ提供システムによっても、第1実施形態のコンテンツ提供システム1と同様の効果が得られる。

【0147】

第4実施形態

第4実施形態は、第19～第24および第28の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図 4 に示す管理装置 1 2 によるディスク I D の生成処理、図 1 8 に示すディスク I D の検証処理、図 1 9 に再生処理におけるコンテンツ復号データの取得処理を除いて、第 1 実施形態のコンテンツ提供システム 1 と同じである。

以下、本実施形態における管理装置 1 2 c のディスク I D 生成方法を説明する。

。

図 2 6 は、本実施形態のコンテンツ提供システムにおいて管理装置 1 2 c が行うディスク I D の生成方法を説明するためのフローチャートである。

図 2 6 に示す各処理は、コントローラ 2 7 がプログラム P R G 1 c を実行することによって実現され、この場合にプログラム P R G 1 c が第 2 0 の発明に対応する。

また、コントローラ 2 7 が図 2 6 に示す各ステップを実行することで、第 2 1 の発明の第 1 の手段および第 2 の手段が実現される。この場合に、管理装置 1 2 c が第 2 0 および第 2 1 の発明のデータ処理装置に対応している。

なお、図 2 6 に示す処理の全部または一部は、コントローラ 2 7 がプログラム P R G 1 c を実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

【 0 1 4 8 】

ステップ S T 3 0 1 :

管理装置 1 2 c のコントローラ 2 7 が、R S A 暗号に用いるのに安全とされる程度に大きな素数 q_1 , q_2 を選択する。

ステップ S T 3 0 2 :

コントローラ 2 7 が、ステップ S T 3 0 1 で選択した素数 q_1 , q_2 の積であるデータ M を公開する。

ステップ S T 3 0 1 , S T 3 0 2 の処理はシステムのセットアップ時に一度だけ行えばよい。

【 0 1 4 9 】

ステップ S T 3 0 3 :

コントローラ 2 7 が、各タイトルに対して、 $S \in Z^*_M$ (S は巡回群 Z^*_M の

生成元) を満たすデータ S をランダムに選択する。当該データ S がディスク ID から導出される値となる。

ステップ ST 3 0 4 :

コントローラ 2 7 が、コンテンツ製作者から、コンテンツのタイトルと製造するディスク型記録媒体 2 b 予定最大生産枚数 W を受け取る。

ステップ ST 3 0 5 :

コントローラ 2 7 が、 $e(w) \in Z^*_M$ ($e(w)$ は巡回群 Z^*_M の生成元) を満たす互いに異なるデータ $e(w)$ 選択する。

ここで、 $e(w)$ と $\lambda(M)$ とは互いに素、すなわち、 $e(w)$ と $\lambda(M)$ の最大公約数が 1 となる。なお、 $\lambda(M)$ は素数 $(q_1 - 1)$ と $(q_2 - 1)$ との最少公倍数である。

【0 1 5 0】

ステップ ST 3 0 6 :

コントローラ 2 7 が、 $(S^{d(w)} \bmod M)$ を演算して、その結果であるデータ $I(w)$ を得る。

ここで、 $d(w)$ は、上記 $\lambda(M)$ を法としたときの上記 $e(w)$ の逆数である。すなわち、 $d(w) = e(w)^{-1} \bmod \lambda(M)$ となる。

ステップ ST 3 0 7 :

コントローラ 2 7 は、 w 番目のディスク ID (w) として、ステップ ST 3 0 5 で決定したデータ $e(w)$ と、ステップ ST 3 0 6 で得たデータ $I(w)$ との組 $(e(w), I(w))$ をディスク ID (w) としてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置 1 4 は、図 6 を用いて前述した手順で、上記ディスク ID (w) を記録したディスク型記録媒体 2 c (第 2 8 の発明の記録媒体) を製造する。

また、ディスク製造装置 1 4 は、上述したステップ ST 3 0 3 で選択したデータ S をコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータ ECONT を生成し、これをディスク型記録媒体 2 c に記録する。

【0 1 5 1】

以下、本実施形態における再生装置 1 5 c の動作例を説明する。

図 2 7 は、再生装置 1 5 c の動作例を説明するための図である。

図 2 7 に示すステップ S T 3 1 2 が第 2 2 の発明の第 1 の工程に対応し、ステップ S T 3 1 6 が第 2 2 の発明の第 2 の工程に対応する。

また、コントローラ 8 7 がステップ S T 3 1 2 を実行することで第 2 4 の発明の第 1 の手段が実現され、ステップ S T 3 1 6 を実行することで第 2 4 の発明の第 2 の手段が実現される。

また、図 2 7 に示す各ステップは、再生装置 1 5 c のコントローラ 8 7 が、プログラム P R G 3 c (第 2 3 の発明のプログラム) を実行することで実現される。

【 0 1 5 2 】

ステップ S T 3 1 1 :

再生装置 1 5 c は、所定のアクセス位置にディスク型記録媒体 2 c がセットされると、記録媒体インタフェース 8 9 を介して、ディスク型記録媒体 2 c からディスク I D を読み出し、これをメモリ 8 8 に格納する。

ステップ S T 3 1 2 :

再生装置 1 5 c のコントローラ 8 7 は、メモリ 8 8 に記録したディスク I D 内のデータ $e(w)$ と $I(w)$ とを用いて、 $I(w)e(w) \bmod M$ を算出し、その結果をデータ S' とする。

ステップ S T 3 1 3 :

コントローラ 8 7 は、記録媒体インタフェース 8 9 を介して、ディスク型記録媒体 2 c からリボケーションリスト D I R L を読み出す。

そして、コントローラ 8 7 は、当該読み出したリボケーションリスト D I R L の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵 (公開鍵) によって検証する。また、改竄検証値としてメッセージ認証コード M A C が付与されている場合は、先に図 8 を参照して説明した M A C 検証処理が実行される。

そして、コントローラ 8 7 は、リボケーションリスト D I R L に改竄がないと判定されたことを条件に、当該リボケーションリスト D I R L のバージョンと、

メモリ 88 に既に格納されているリボケーションリスト D I R L とのバージョン比較を実行する。

コントローラ 87 は、当該読み出したリボケーションリスト D I R L のバージョンがメモリ 88 に既に格納されているリボケーションリスト D I R L より新しい場合は、当該読み出したリボケーションリスト D I R L によって、メモリ 88 内のリボケーションリスト D I R L を更新する。

【0153】

ステップ S T 3 1 4 :

コントローラ 87 は、ステップ S T 3 1 1 で読み出したディスク I D がリボケーションリスト D I R L 内に存在するか否かを判断し、存在すると判断するとステップ S T 3 1 5 に進み、そうでない場合にはステップ S T 3 1 6 に進む。

ステップ S T 3 1 5 :

コントローラ 87 は、ディスク型記録媒体 2 c に記録されている暗号化コンテンツデータ E C O N T の再生を停止（禁止）する。

ステップ S T 3 1 6 :

コントローラ 87 は、ディスク型記録媒体 2 c に記録されている暗号化コンテンツデータ E C O N T を読み出し、ステップ S T 3 1 2 で生成したデータ S' を基に取得したコンテンツ鍵データを用いて、暗号化コンテンツデータ E C O N T を復号し、続いて再生する。

コントローラ 87 は、例えば、ルート鍵データと、データ S' との排他的論理和をコンテンツ鍵データとする。

【0154】

本実施形態のコンテンツ提供システムによっても、第 1 実施形態のコンテンツ提供システム 1 と同様の効果が得られる。

【0155】

【発明の効果】

本発明によれば、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第 1 の効果が得ら

れる。

また、本発明によれば、上記第 1 の効果を得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第 2 の効果が得られる。

また、本発明によれば、上記第 1 の効果を得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを記録した記録媒体を提供できるという第 3 の効果が得られる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態に係わるディスク型記録媒体に記録されるデータを説明するための図である。

【図 2】

図 2 は、本発明の実施形態に係わるコンテンツ提供システムの全体構成図である。

【図 3】

図 3 は、図 2 に示す管理装置の構成図である。

【図 4】

図 4 は、図 3 に示す管理装置によるディスク ID の生成処理を説明するためのフローチャートである。

【図 5】

図 5 は、図 2 に示すディスク製造装置の構成図である。

【図 6】

図 6 は、図 5 に示すディスク製造装置によるディスク製造手順を説明するためのフローチャートである。

【図 7】

図 7 は、図 1 に示すディスク型記録媒体に記録されるリボケーションリスト D I R L のデータ構成を説明する図である。

【図 8】

図 8 は、MAC 値生成処理例を示す図である。

【図 9】

図 9 は、各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

【図 10】

図 10 は、各種キー、データの配布に使用される有効化キープブロック (EKB) の例を示す図である。

【図 11】

図 11 は、コンテンツ鍵の有効化キープブロック (EKB) を使用した配布例と復号処理例を示す図である。

【図 12】

図 12 は、有効化キープブロック (EKB) のフォーマット例を示す図である。

【図 13】

図 13 は、有効化キープブロック (EKB) のタグの構成を説明する図である。

【図 14】

図 14 は、ツリー構成におけるカテゴリ分割を説明する図である。

【図 15】

図 15 は、ツリー構成におけるカテゴリ分割を説明する図である。

【図 16】

図 16 は、図 2 に示す再生装置の構成図である。

【図 17】

図 17 は、図 16 に示す再生装置の再生処理を説明するためのフローチャートである。

【図 18】

図 18 は、図 17 に示すステップ S T 3 2 のディスク I D の検証処理を説明するためのフローチャートである。

【図 19】

図 19 は、図 17 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

【図 20】

図 20 は、本発明の第 2 実施形態における管理装置のディスク ID の生成処理を説明するためのフローチャートである。

【図 21】

図 21 は、本発明の第 2 実施形態における再生装置による図 17 に示すステップ S T 3 2 のディスク ID の検証処理を説明するためのフローチャートである。

【図 22】

図 22 は、本発明の第 2 実施形態における再生装置による図 17 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

【図 23】

図 23 は、本発明の第 3 実施形態における管理装置のディスク ID の生成処理を説明するためのフローチャートである。

【図 24】

図 24 は、本発明の第 3 実施形態における再生装置による図 17 に示すステップ S T 3 2 のディスク ID の検証処理を説明するためのフローチャートである。

【図 25】

図 25 は、本発明の第 3 実施形態における再生装置による図 17 に示すステップ S T 3 8 の再生処理を説明するためのフローチャートである。

【図 26】

図 26 は、本発明の第 4 実施形態における管理装置のディスク ID の生成処理を説明するためのフローチャートである。

【図 27】

図 27 は、本発明の第 4 実施形態における再生装置による再生処理を説明するためのフローチャートである。

【符号の説明】

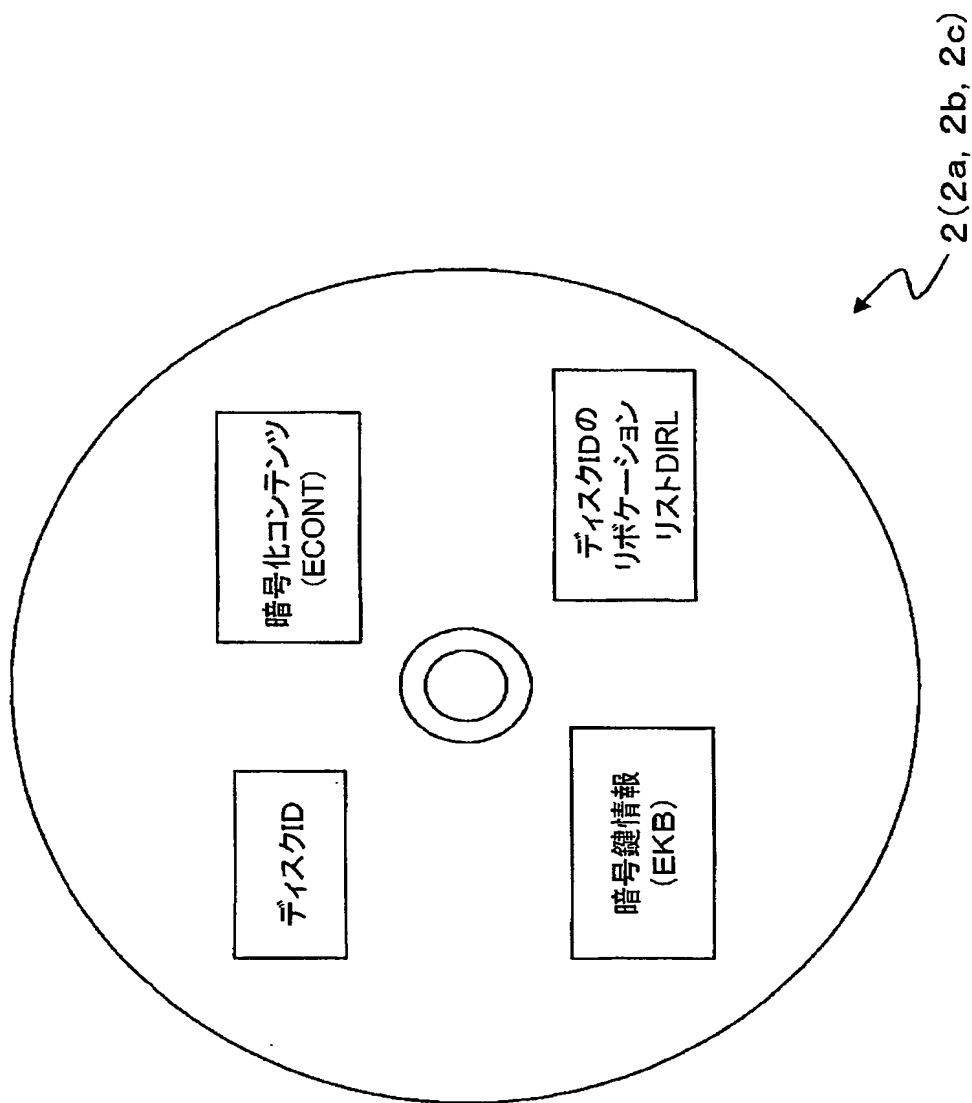
2, 2 a, 2 b, 2 c…ディスク型記録媒体、12, 12 a, 12 b, 12 c…管理装置、13…コンテンツ提供装置、14…ディスク製造装置、15, 15 a, 15 b, 15 c…再生装置、21…バス、22…メインメモリ、23…セキュアメモリ、24…入出力インタフェース、25…記録媒体インタフェース、2

6…演算ユニット、27…コントローラ、80…バス、81…入出力インタフェース、82…コーデック、83…入出力インタフェース、84…コンバータ、85…暗号処理部、86…ROM、87…コントローラ、88…メモリ、89…記録媒体インタフェース

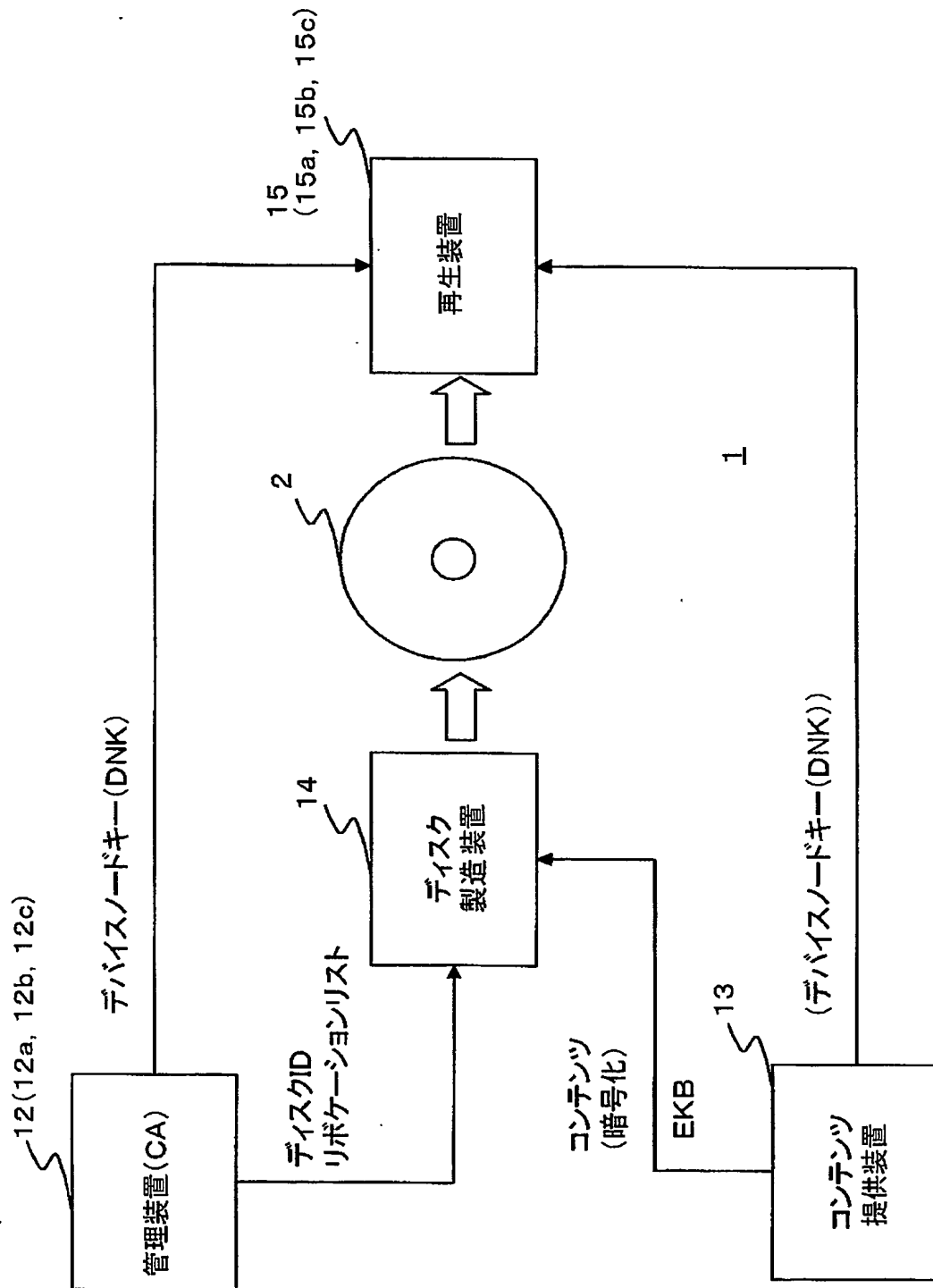
【書類名】

図面

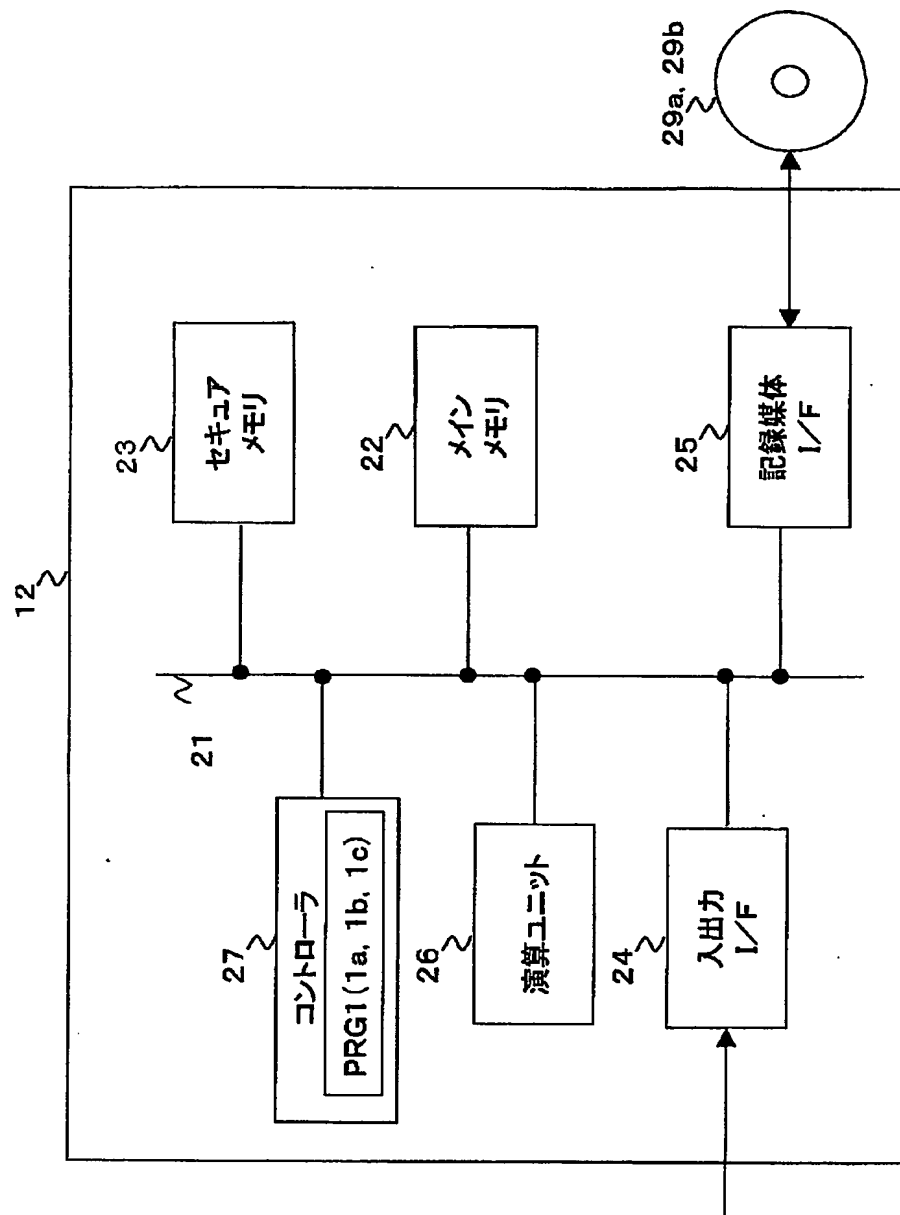
【図 1】



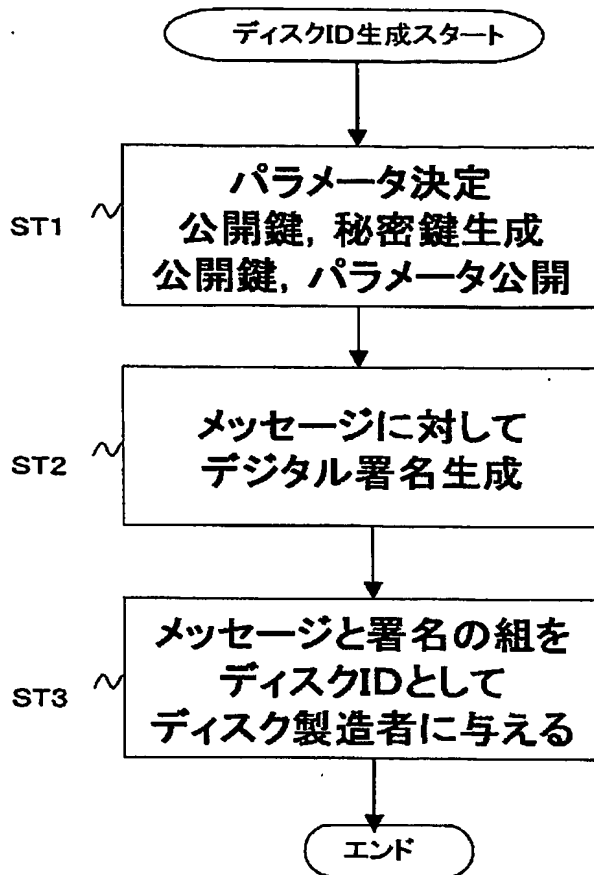
【図 2】



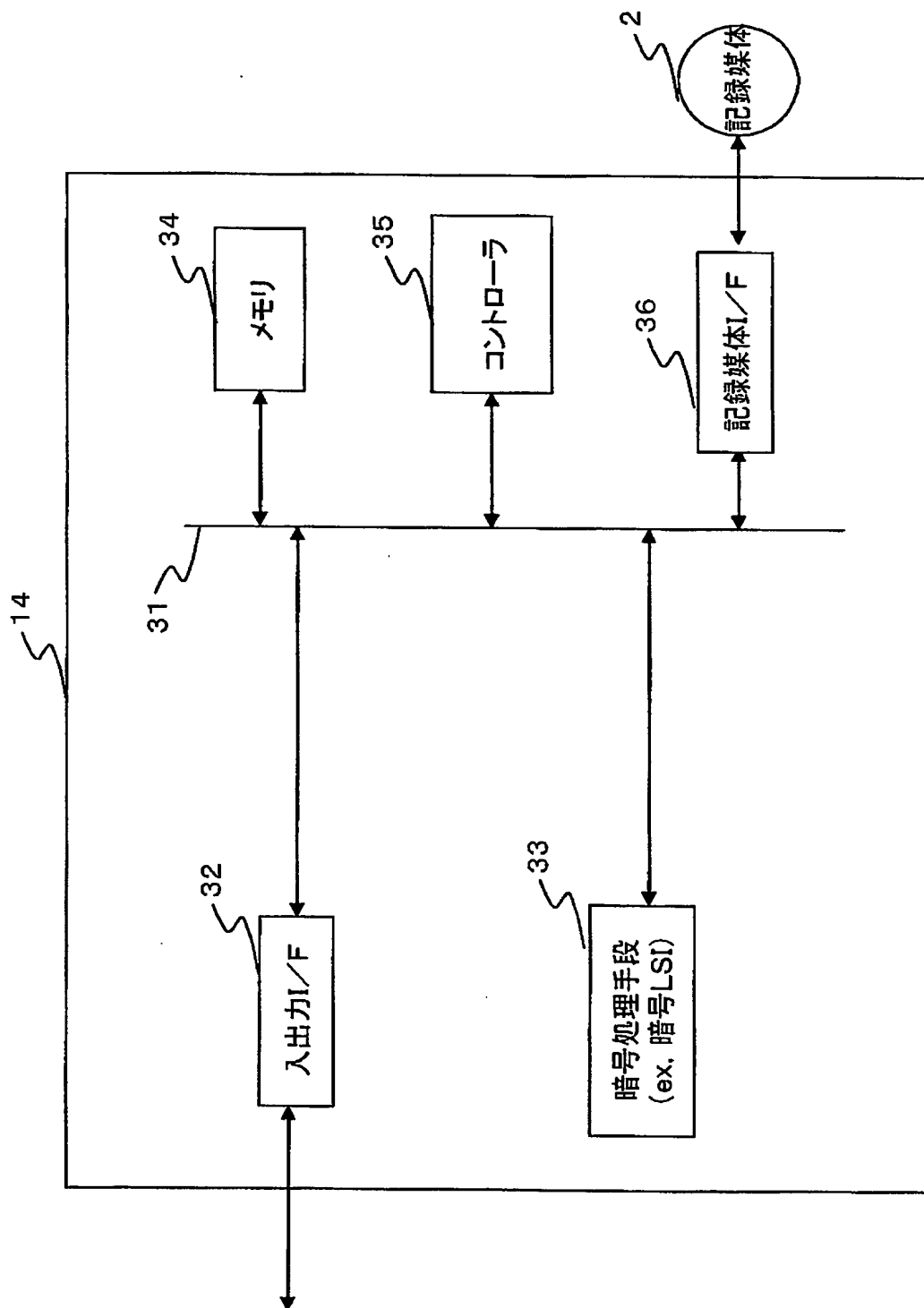
【図 3】



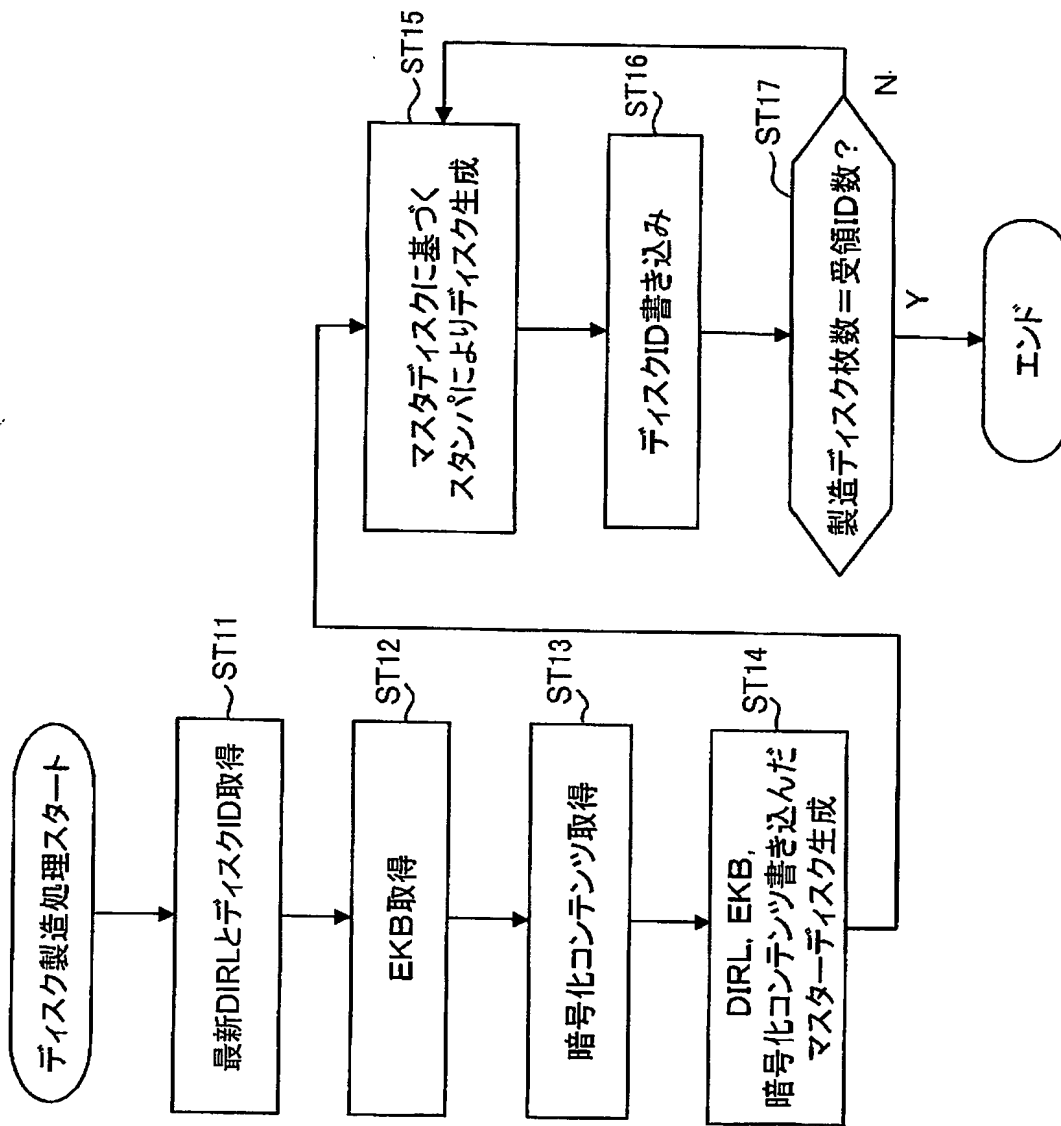
【図 4】



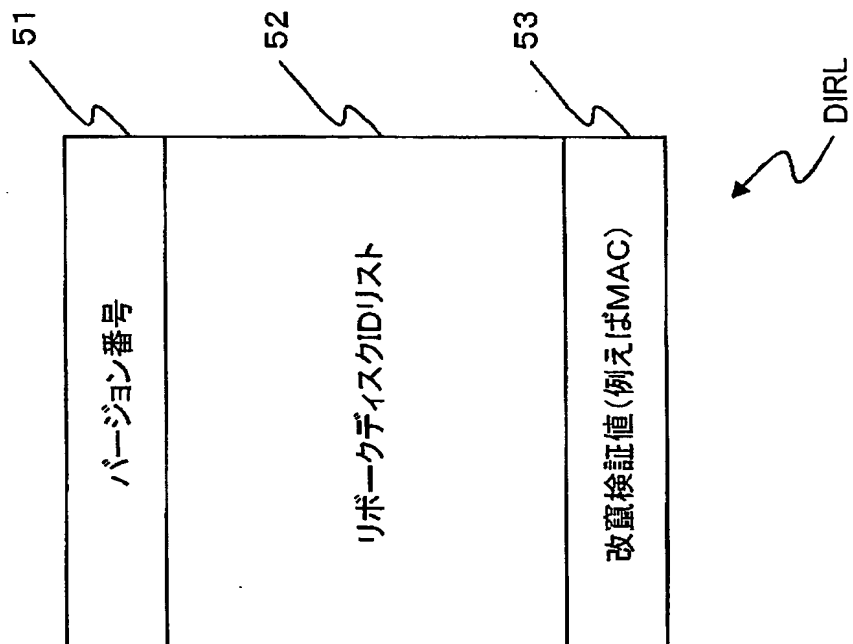
【図 5】



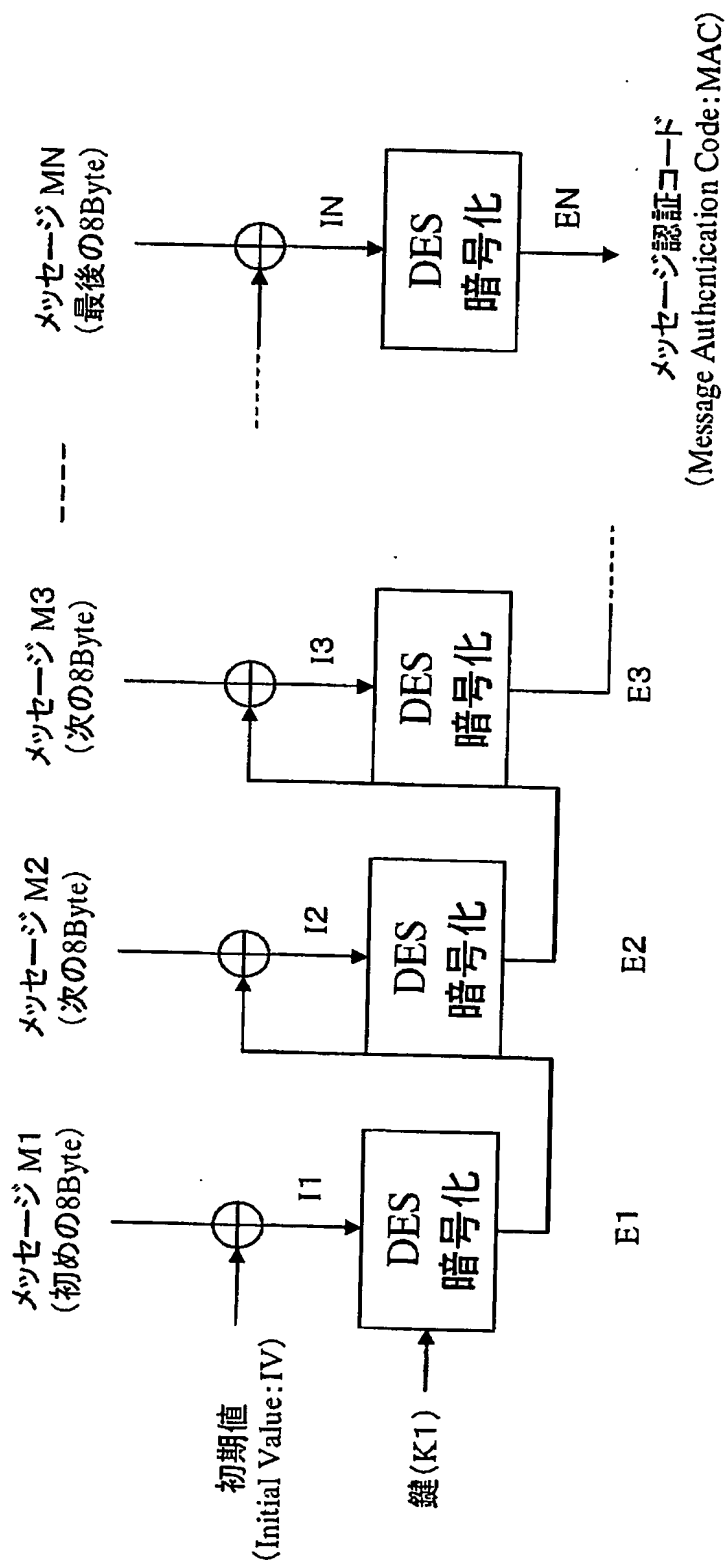
【図6】



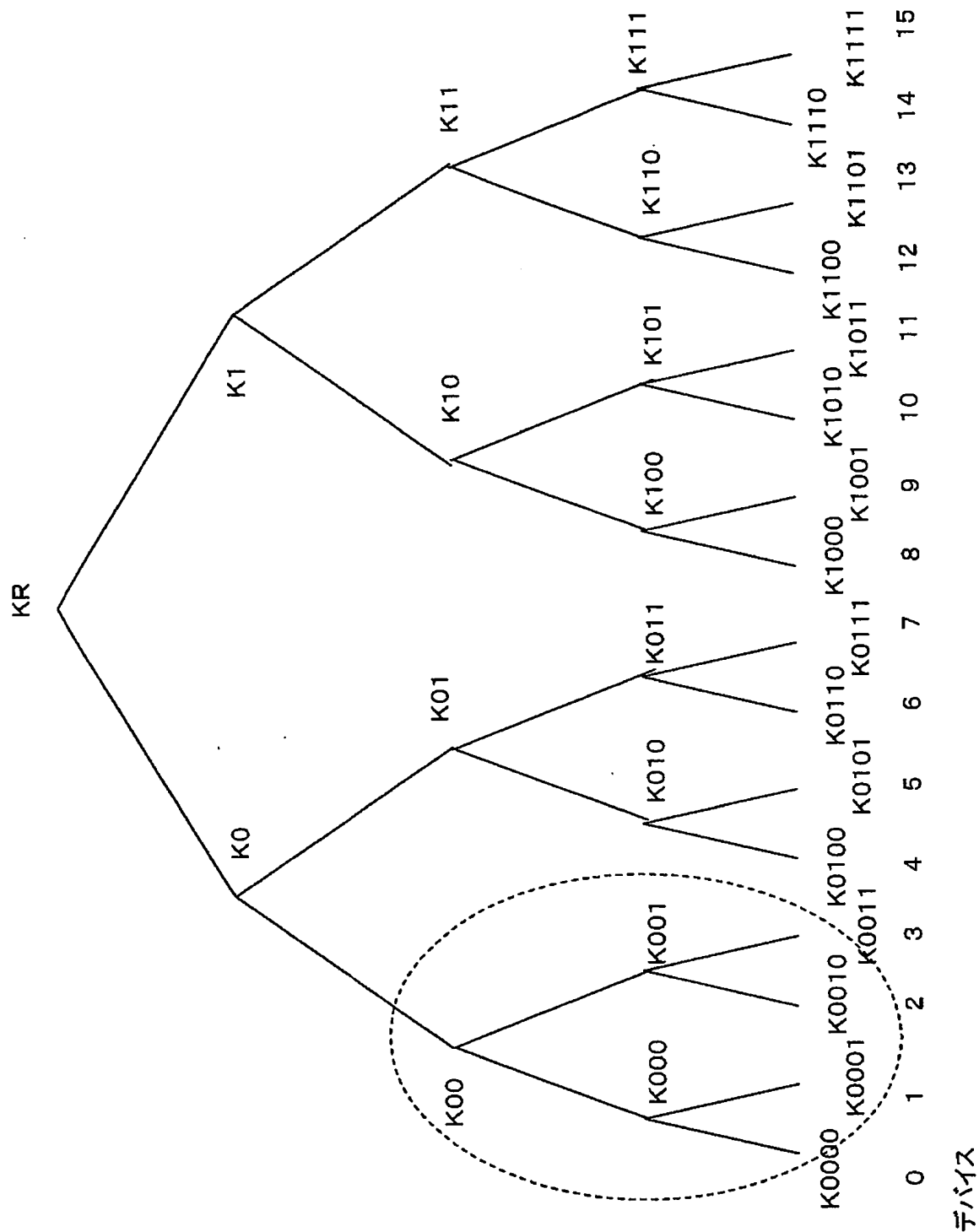
【図 7】



【図 8】



【図 9】



【図 1 0】

(A) 有効化キーブロック

(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version): t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

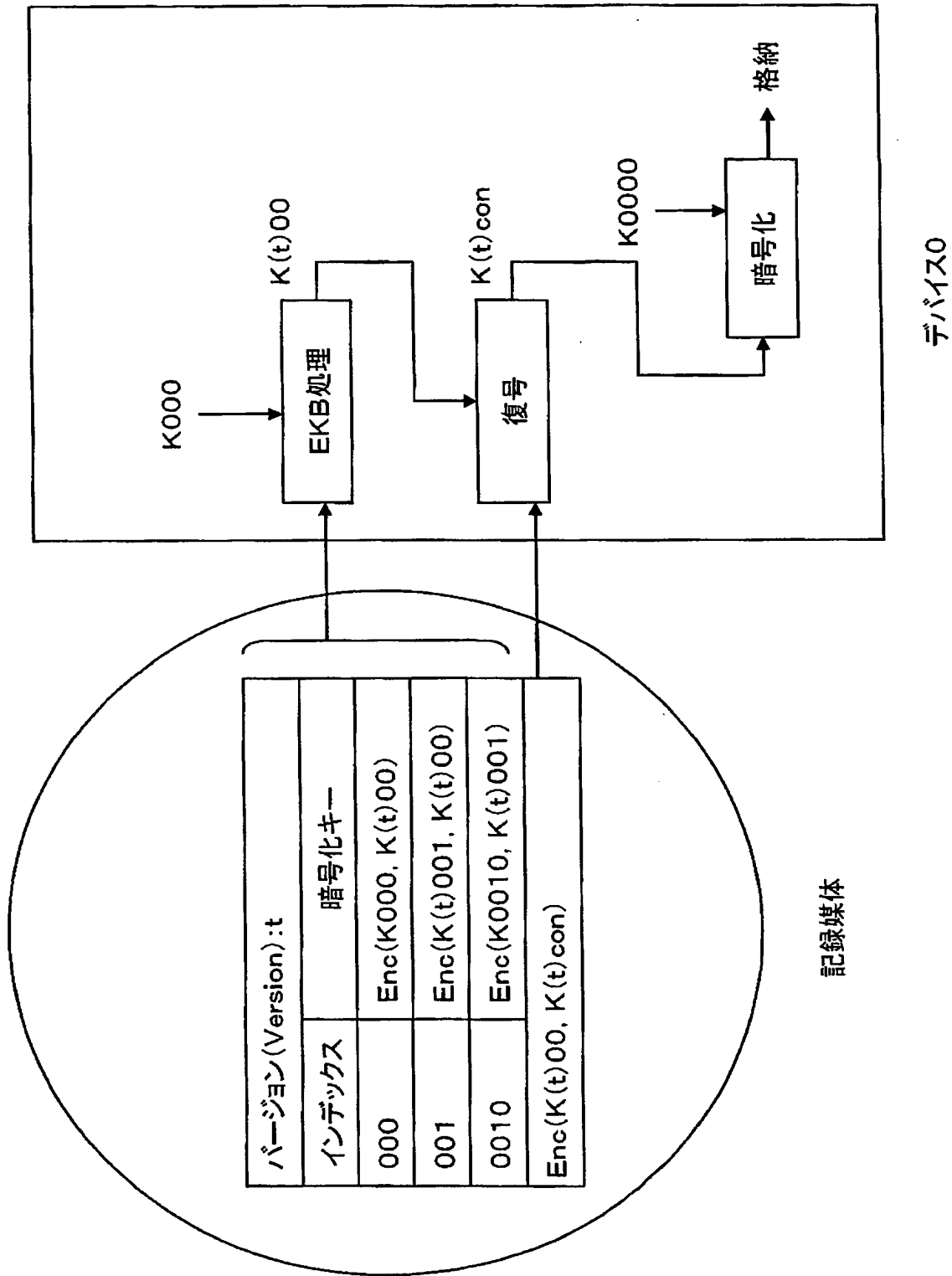
(B) 有効化キーブロック

(EKB:Enabling Key Block) 例2

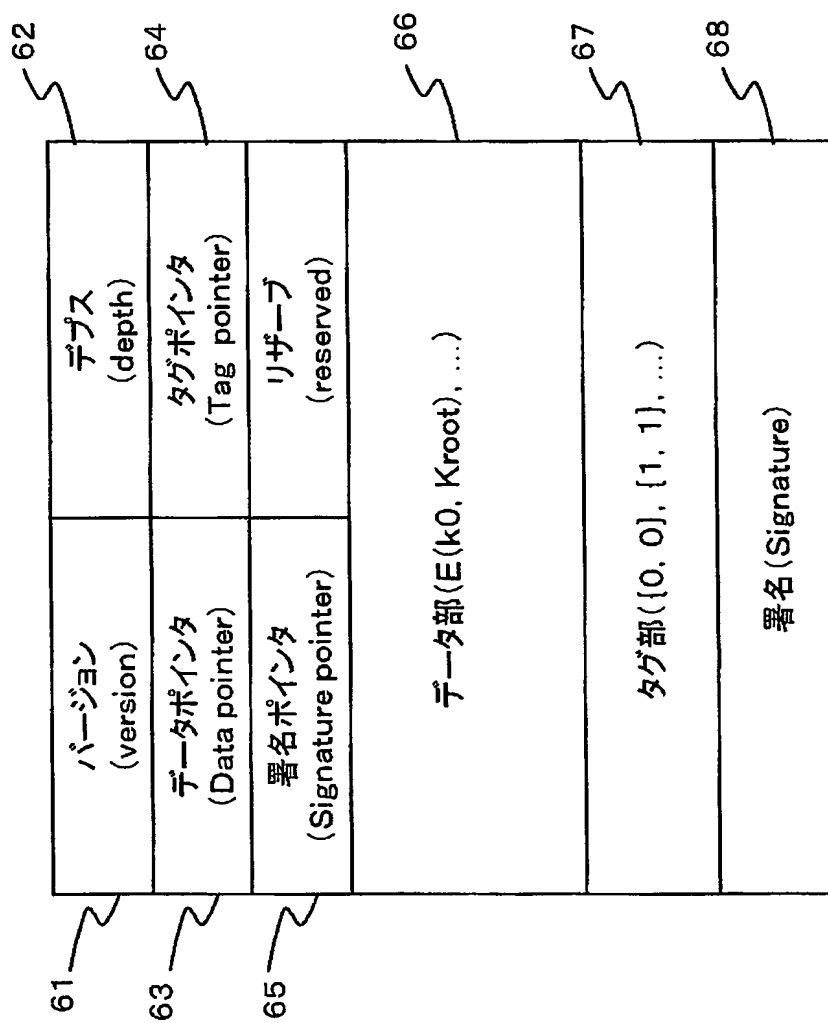
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version): t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

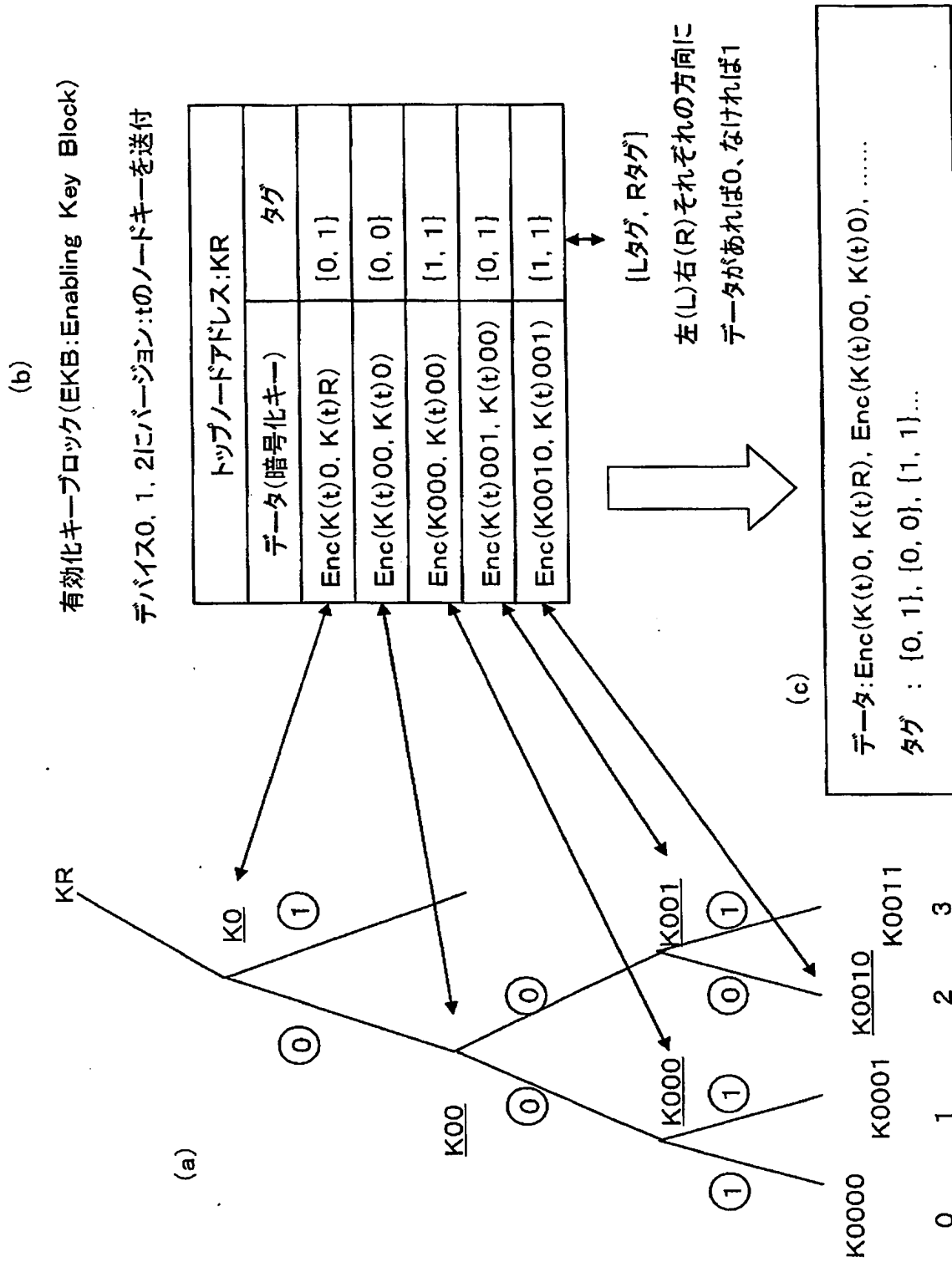
【図 11】



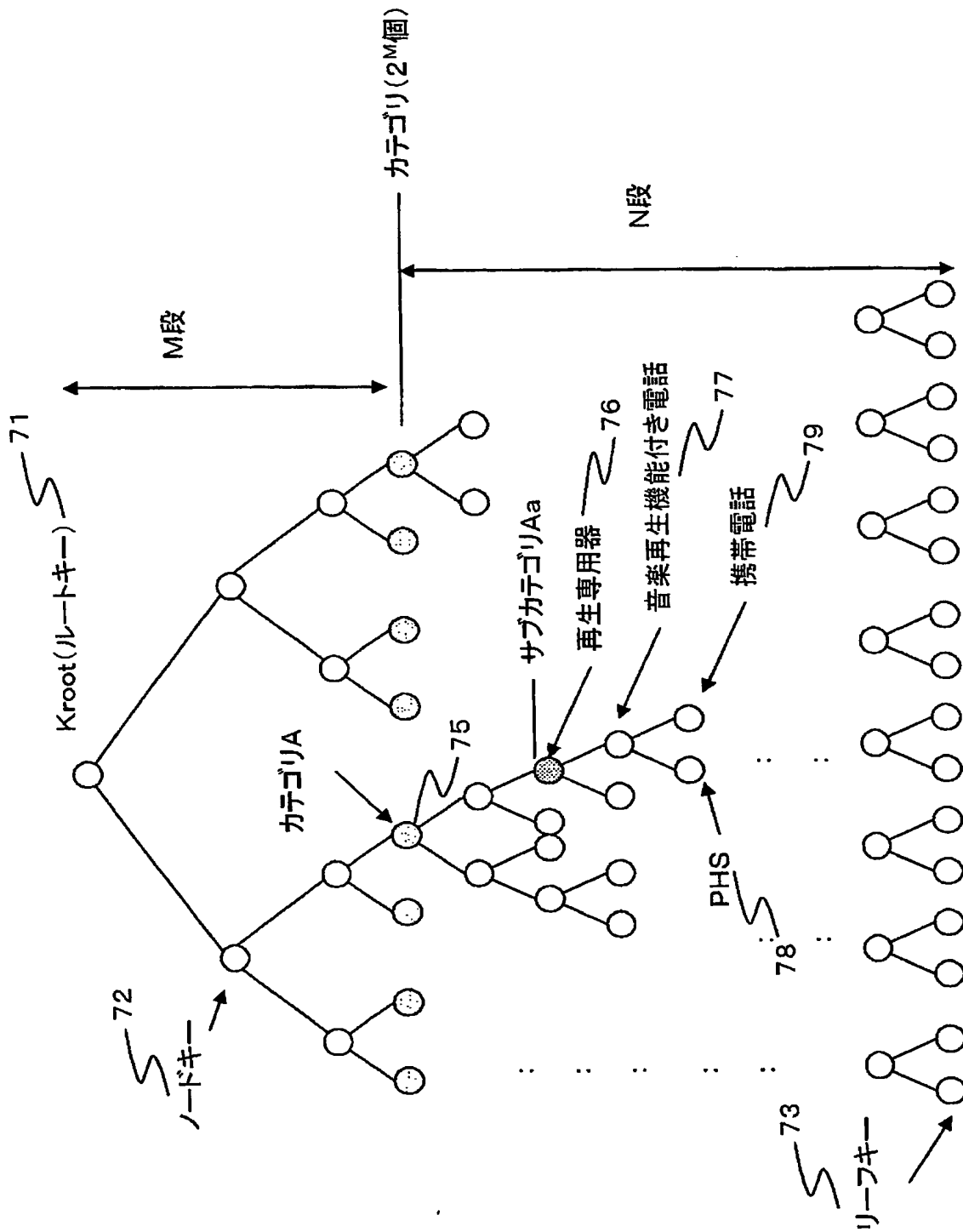
【図 12】



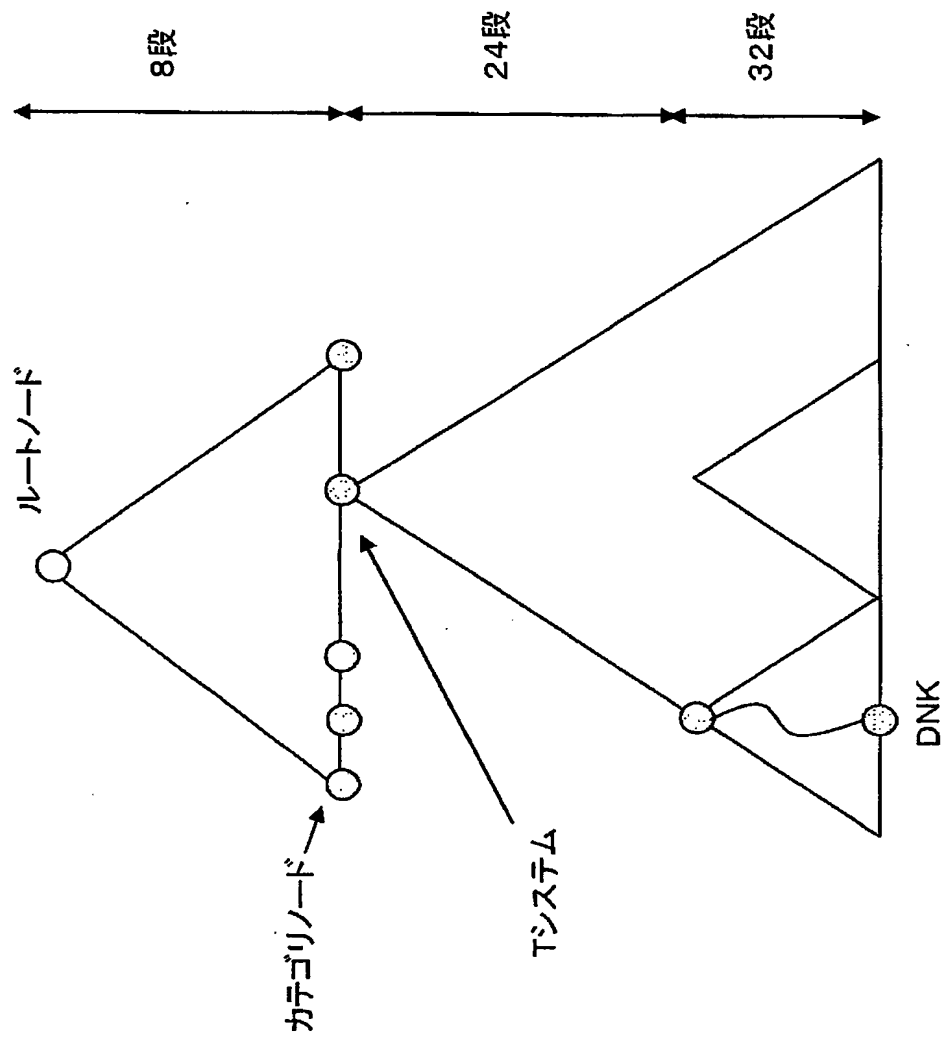
【図 13】



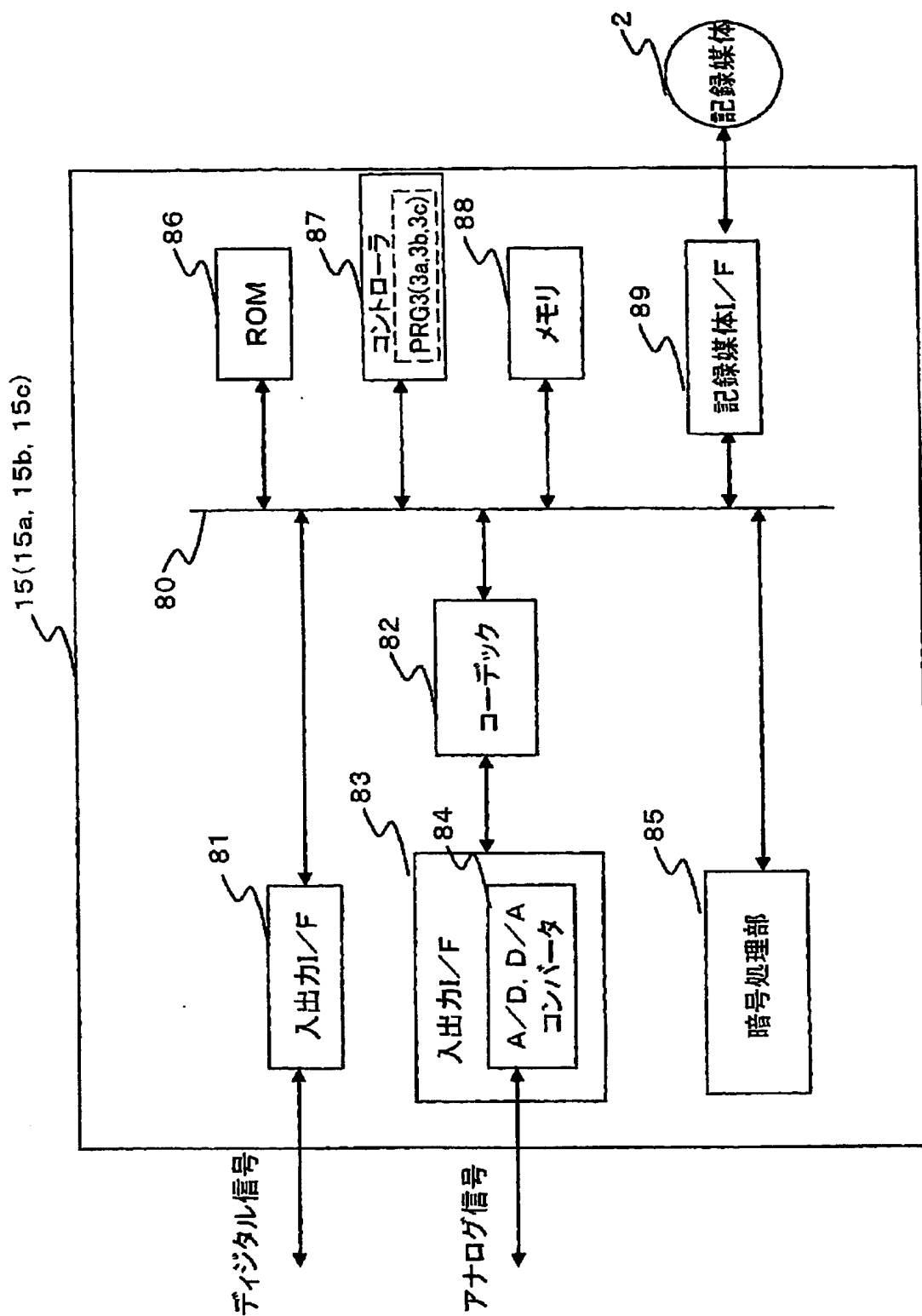
【図 14】



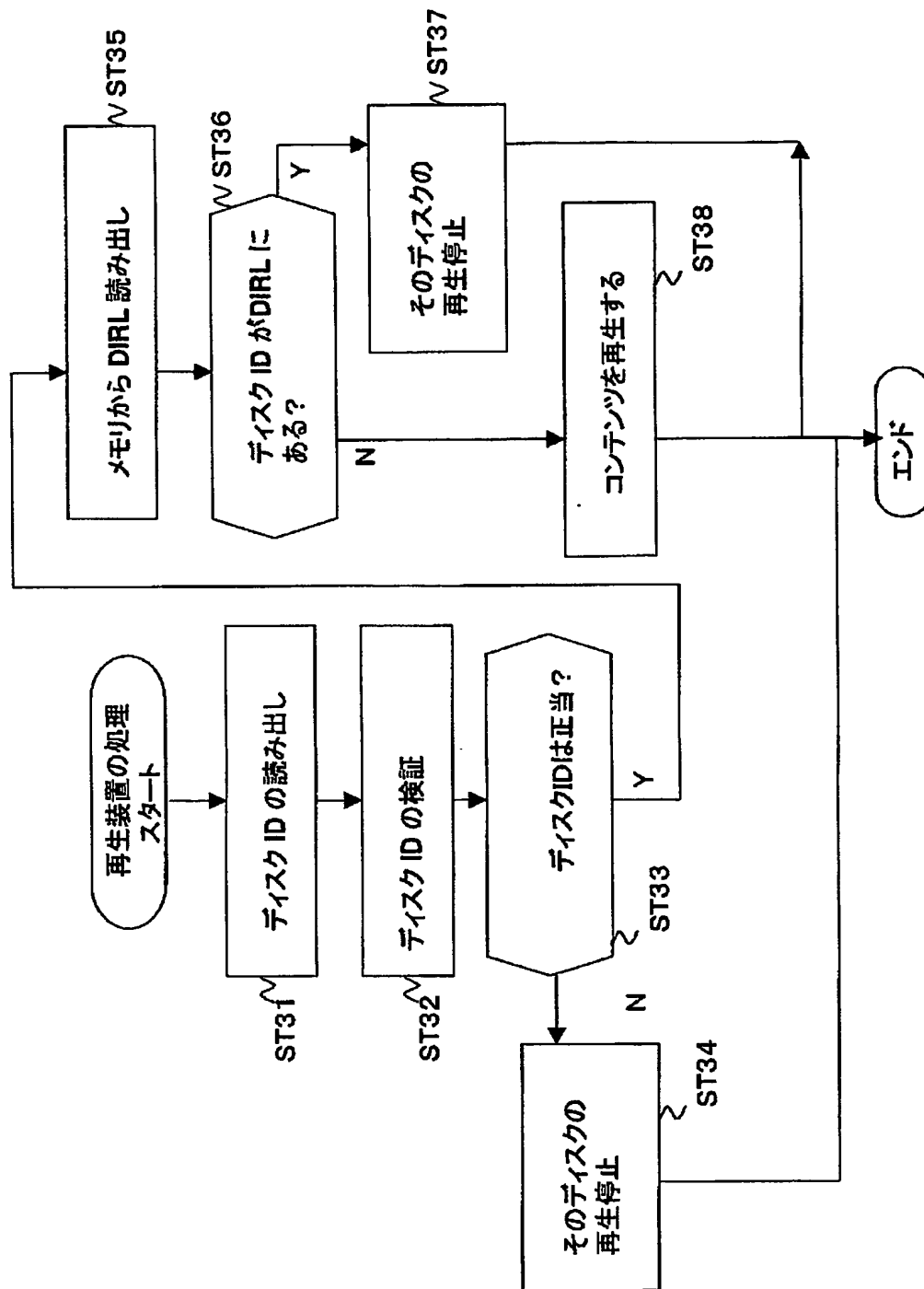
【図 15】



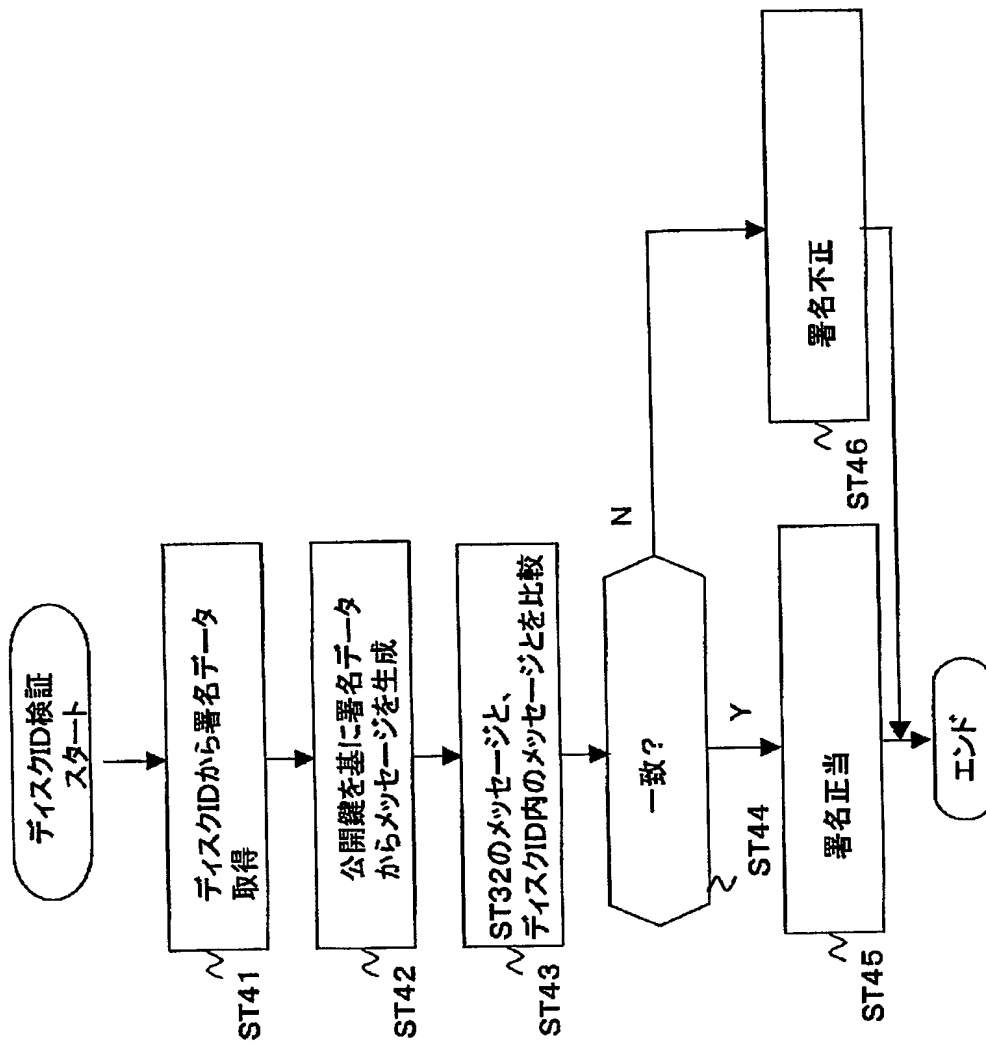
【図16】



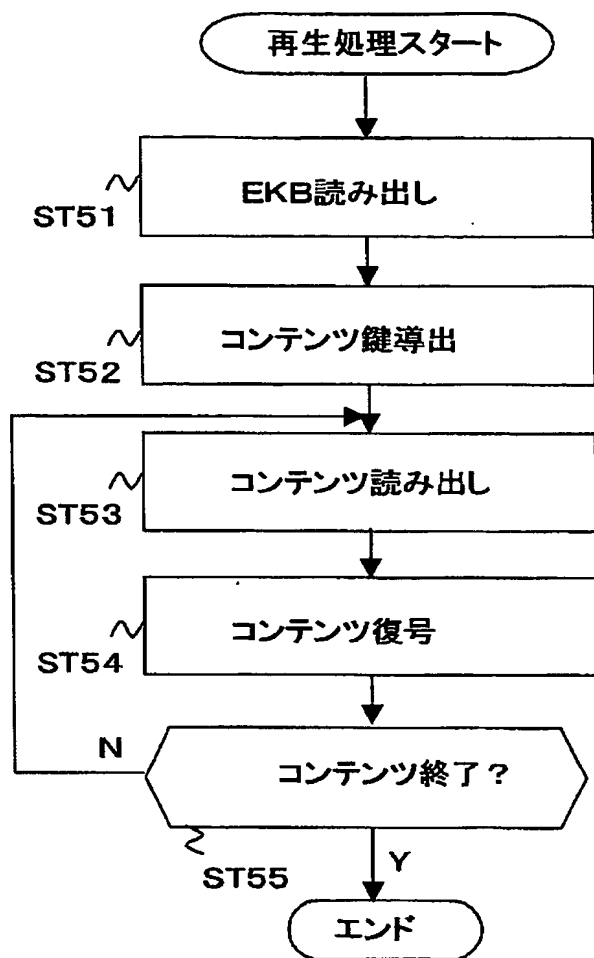
【図 17】



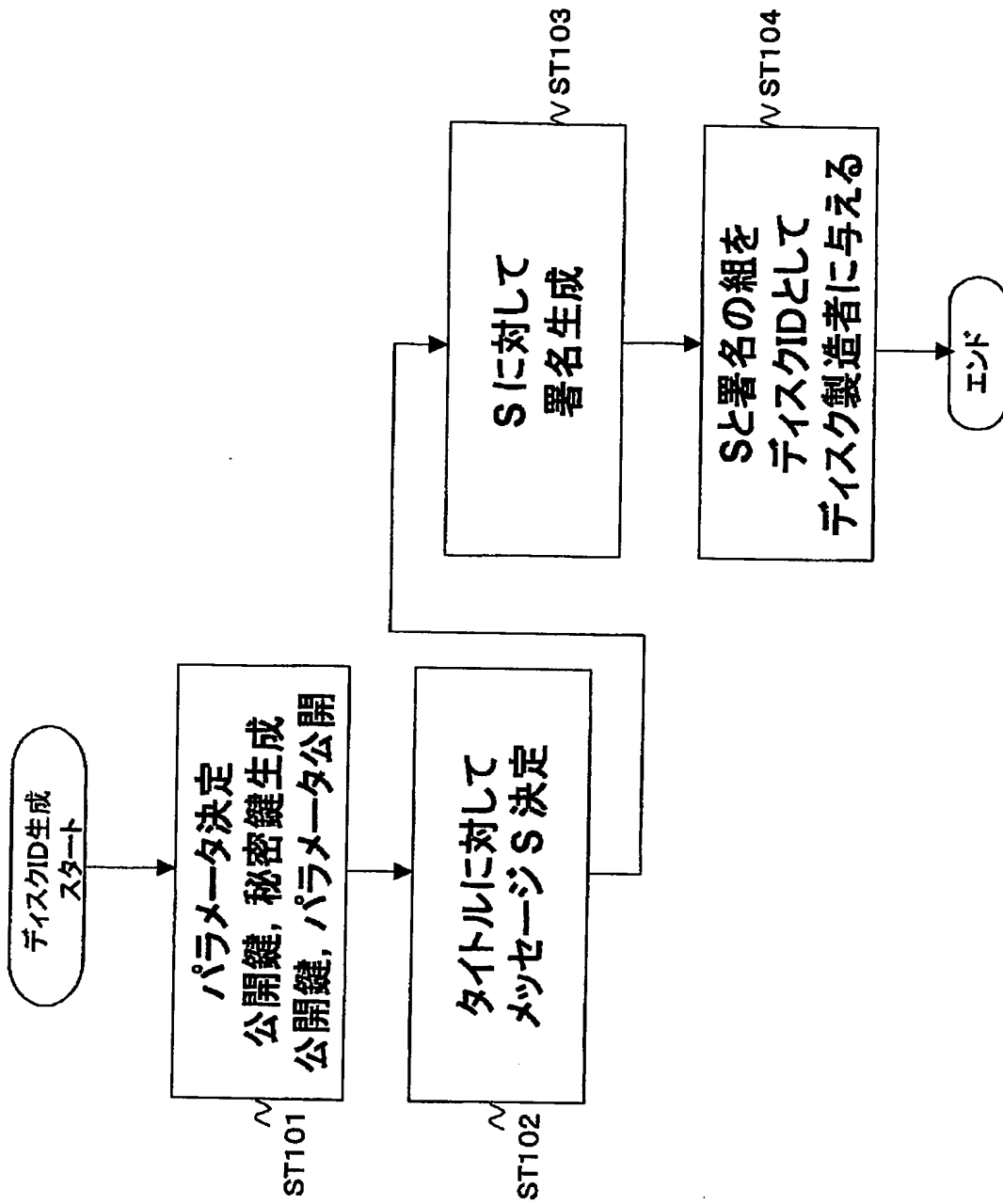
【図 18】



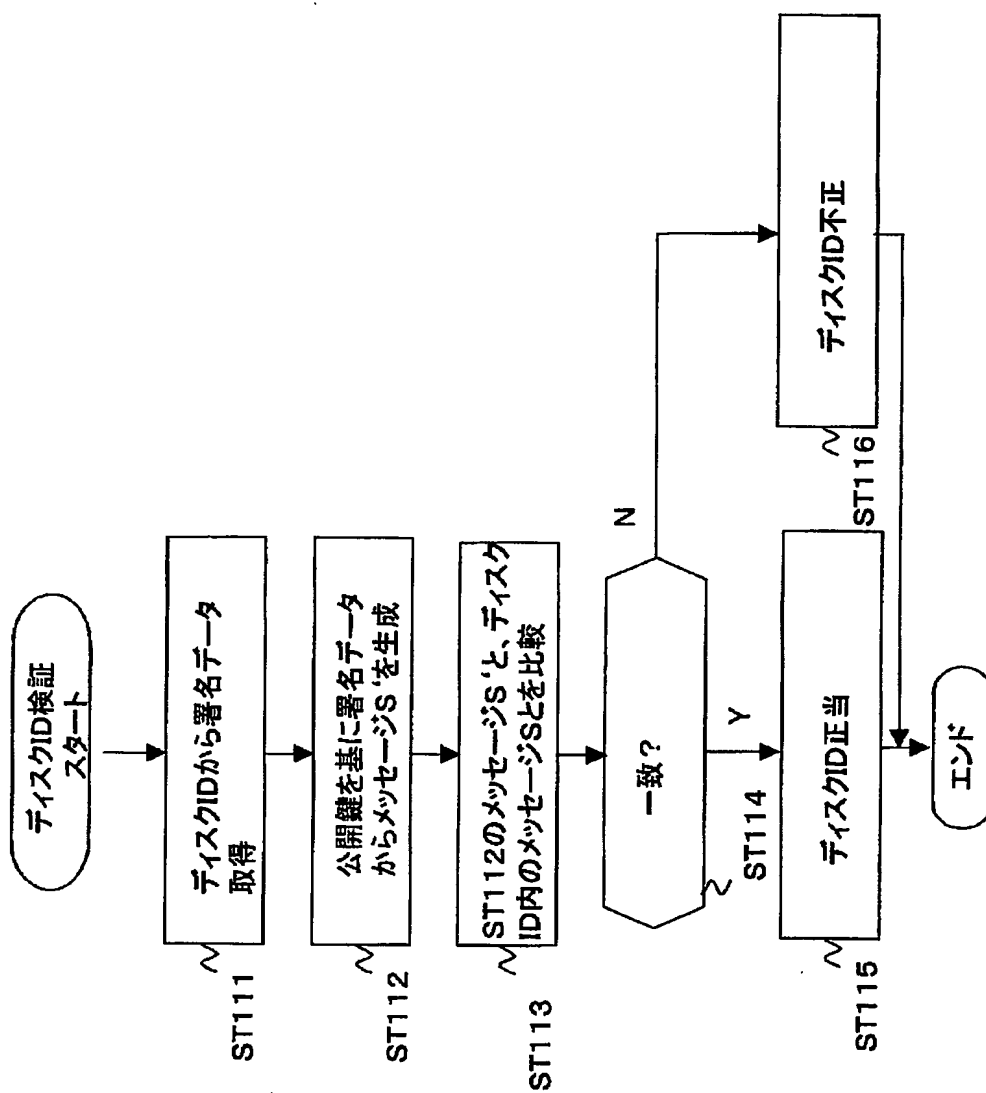
【図 19】



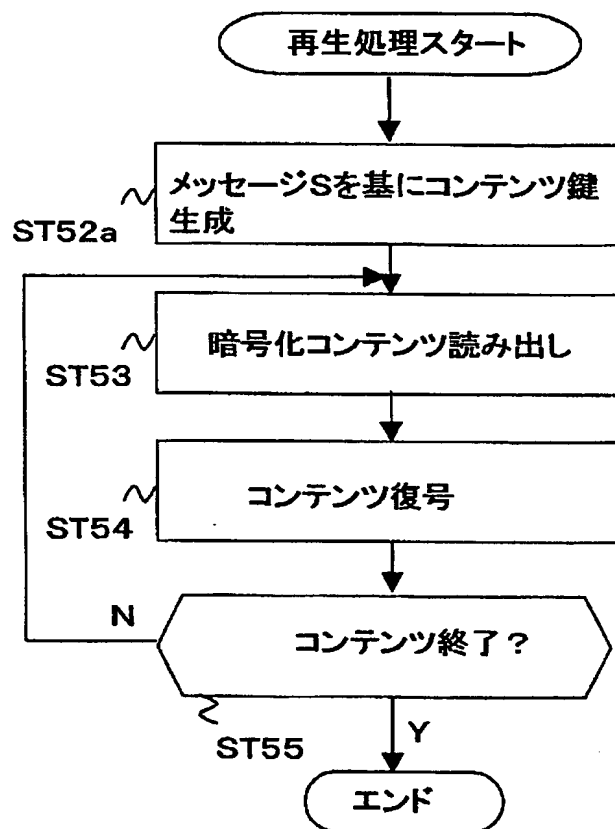
【図 20】



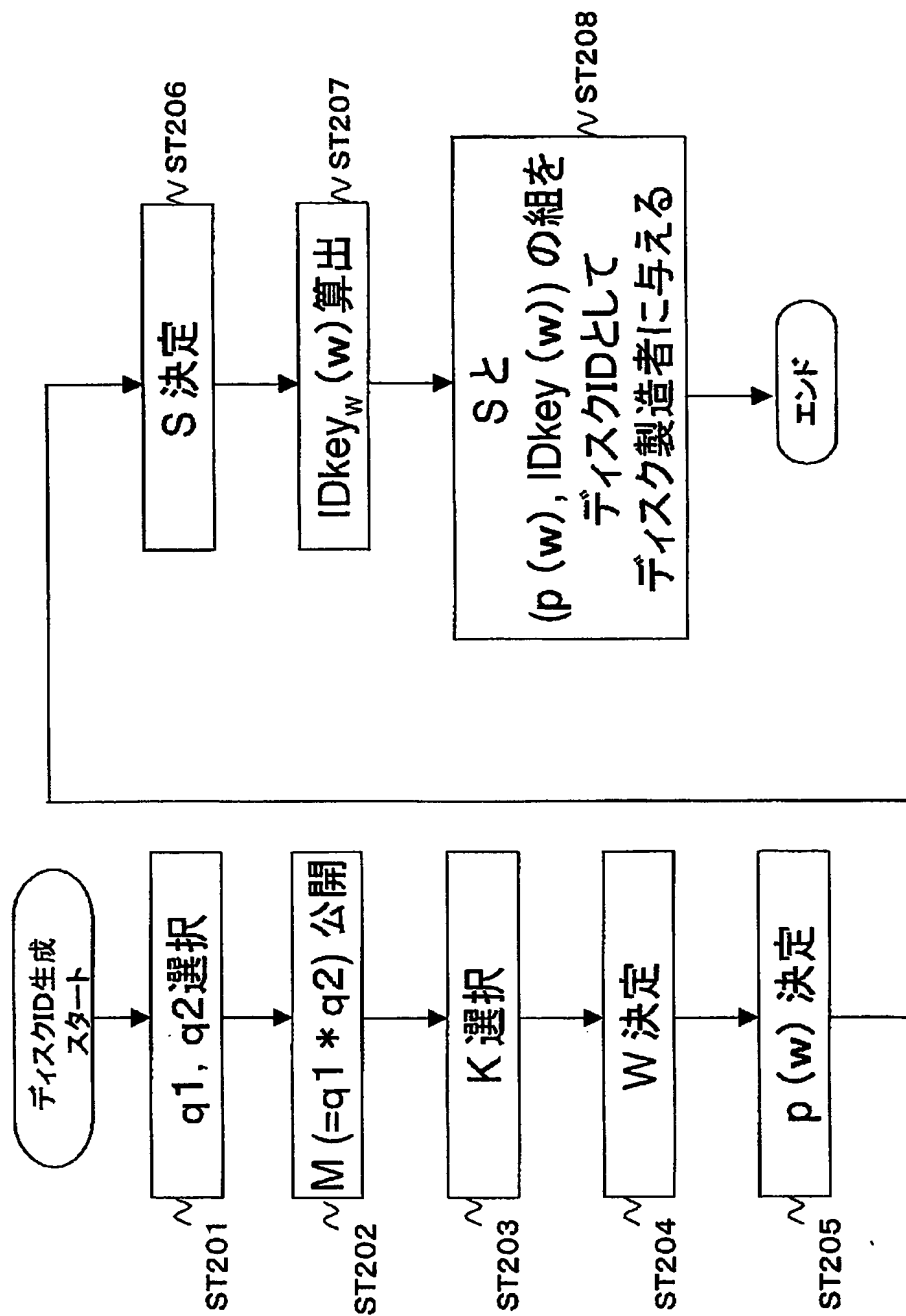
【図 21】



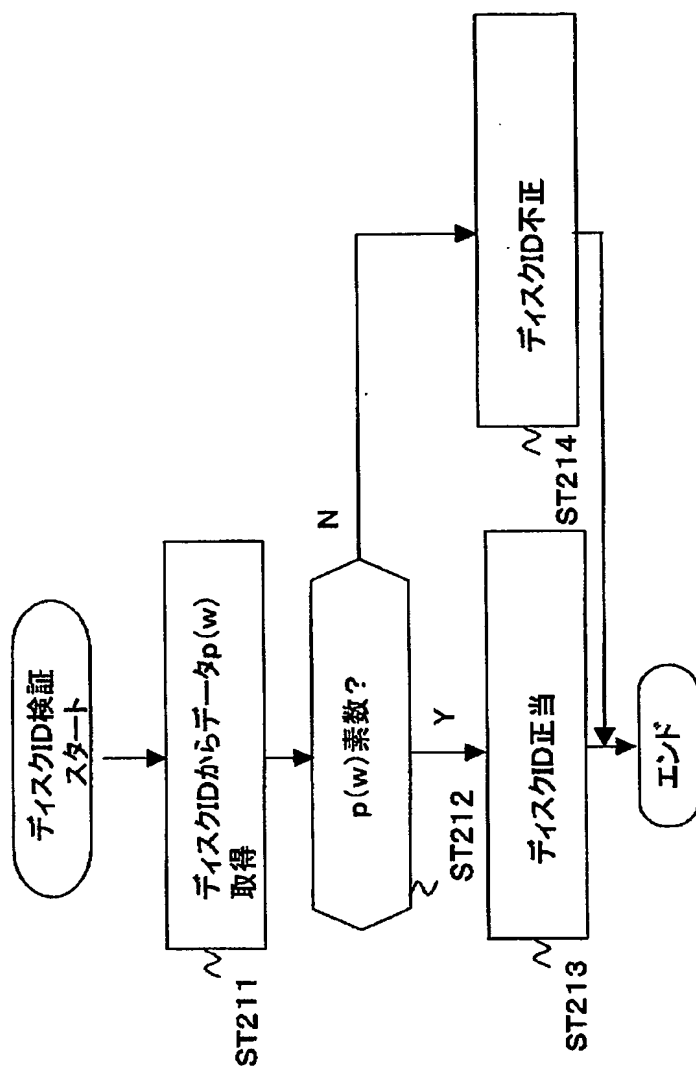
【図 22】



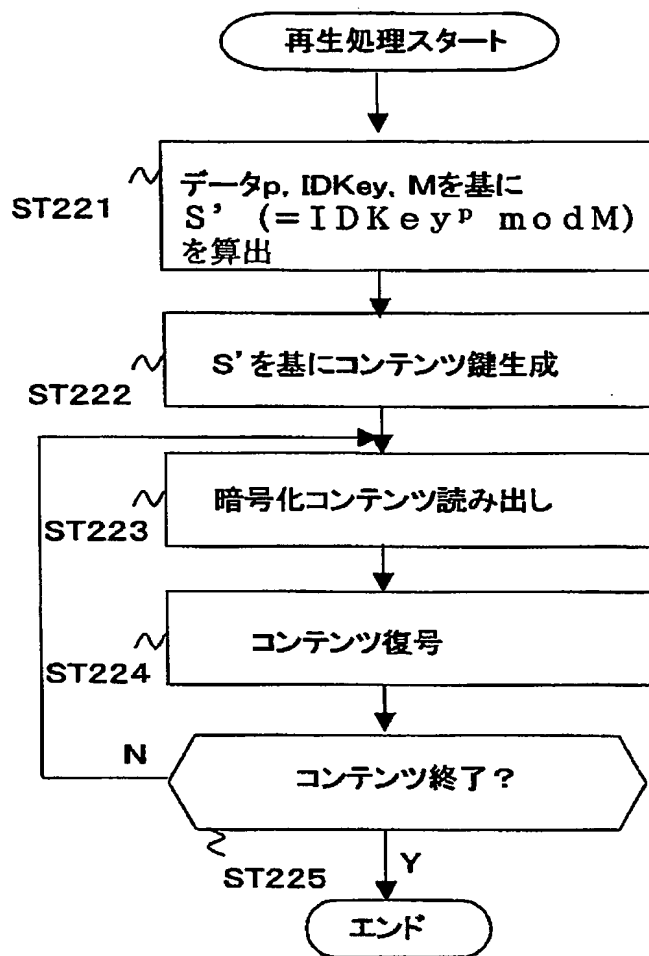
【図 23】



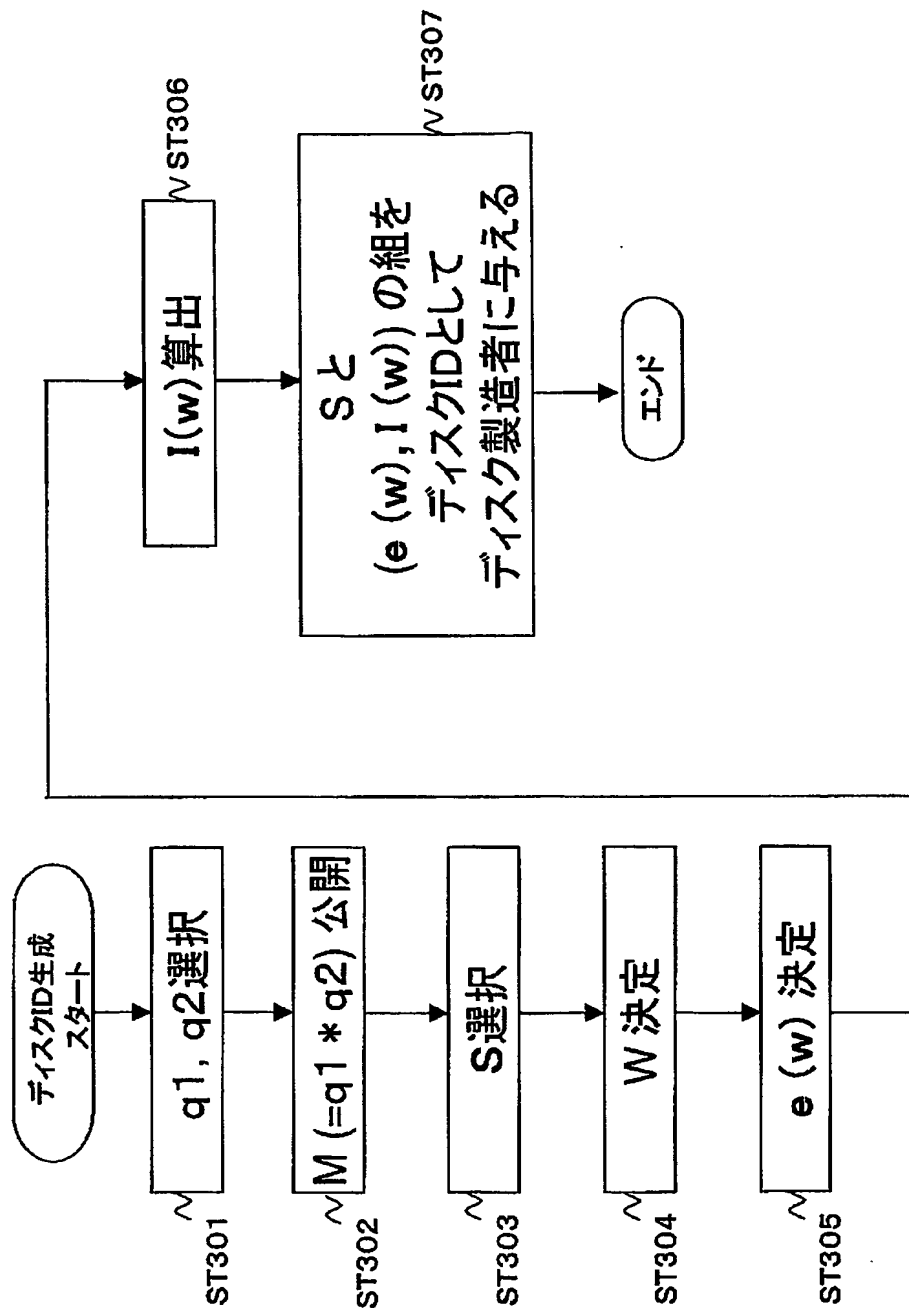
【図 24】



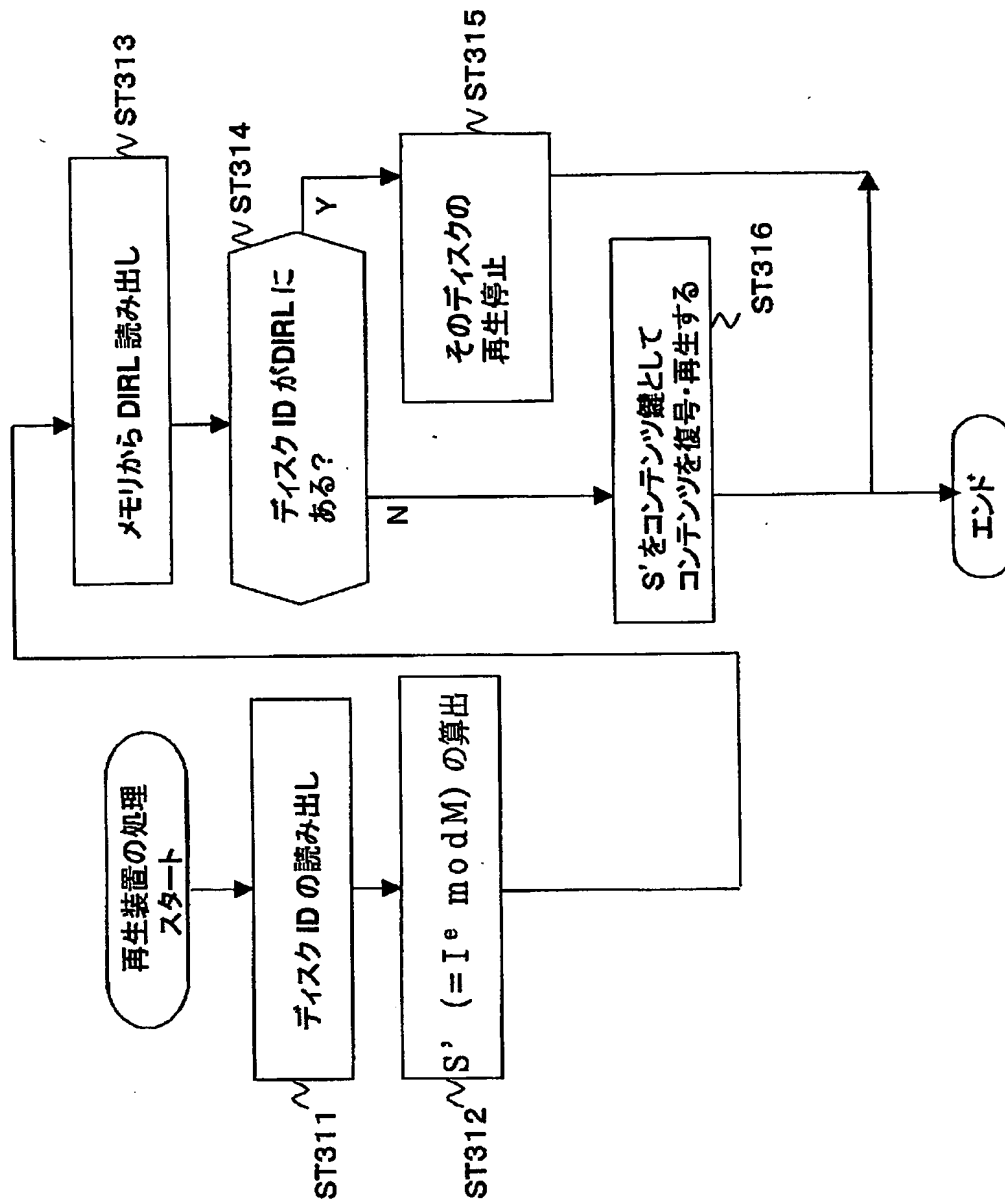
【図 25】



【図 26】



【図 27】



【書類名】 要約書

【要約】

【課題】 識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法を提供する。

【解決手段】 管理装置 12 は、自らの秘密鍵を用いて異なる複数の署名データを生成し、これをディスク ID としてディスク製造装置 14 に提供する。ディスク製造装置 14 は、複数の上記ディスク ID をそれぞれ記録した複数のディスク型記録媒体 2 を製造する。再生装置 15 は、再生装置 15 を再生する前に、ディスク型記録媒体 2 からディスク ID を読み出し、これを管理装置 12 の公開鍵データを基に検証する。

【選択図】 図 2

特願 2003-125968

出願人履歴情報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住所

東京都品川区北品川6丁目7番35号

氏名

ソニー株式会社